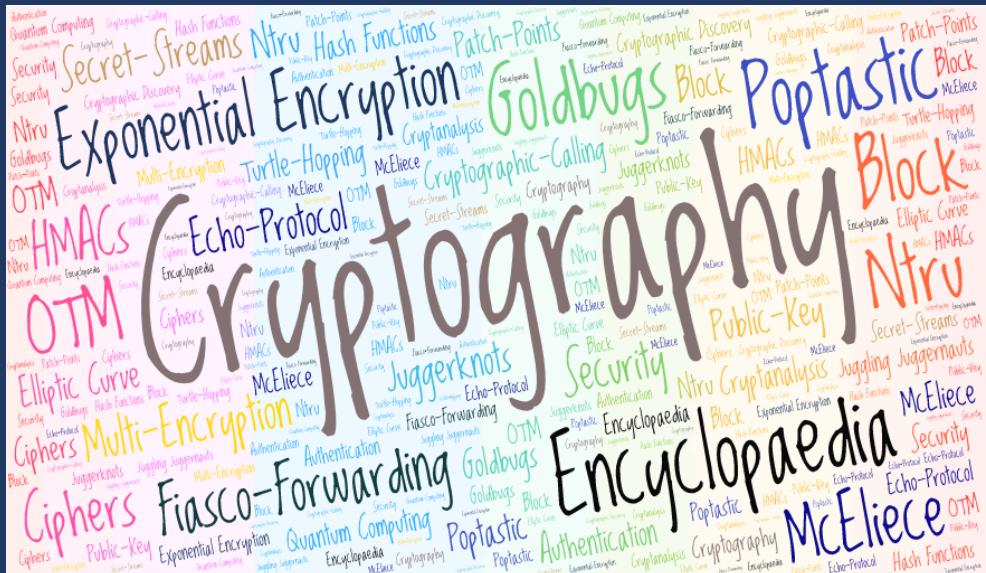


Linda A. Bertram
Gunther van Doobles
et al. *Editors*

Nomenclatura -

Encyclopedia of modern Cryptography and Internet Security



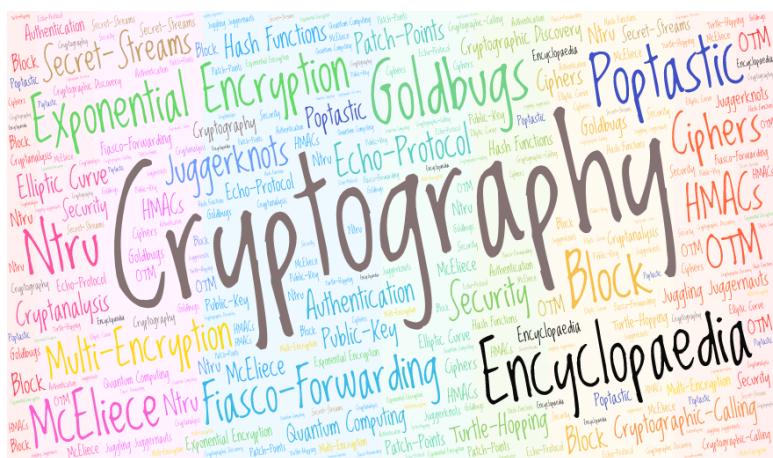
From AutoCrypt and Exponential Encryption to Zero-Knowledge-Proof Keys

Linda A. Bertram
Gunther van Dooble
et al. *Editors*

Nomenclatura -

Encyclopedia of modern Cryptography and Internet Security:

From AutoCrypt and Exponential Encryption to Zero-Knowledge-Proof Keys



Impressum / Paperback:

Bertram, Linda A. / Dooble, Gunther van / et al. (2019) (Eds.):
Nomenclatura - Encyclopedia of modern Cryptography
and Internet Security: From AutoCrypt and Exponential
Encryption to Zero-Knowledge-Proof Keys,
including explanations on Authentication, Block ciphers and
stream ciphers, Cryptanalysis and security, Cryptographic
Calling and Cryptographic Discovery, Cryptographic protocols
like e.g. the Echo-Protocol, Elliptic curve cryptography,
Exponential Encryption, Fiasco Forwarding, Goldbugs, Hash
functions and MACs, juggling Juggernauts and Juggerknot
Keys, McEliece, Multi-Encryption, NTRU, OTM, Public key
cryptography, Patch-Points, POPTASTIC, Quantum
Computing Cryptography, Secret Streams, Turtle Hopping,
Two-Way-Calling and many more...
Norderstedt 2019, ISBN: 9783746066684.

Manufacturer / Publisher / Printing:

BoD, Norderstedt. 2019, <https://www.bod.de>
ISBN: 9783746066684.

More bibliographic info under: <https://portal.dnb.de>

Computer Security - Encyclopedias.

Data Encryption (Computer science) - Encyclopedias.

Cryptographie - Dictionnaire.

Sécurité Informatique - Dictionnaire.

Computer security.

Data encryption (Computer science).

License terms of referenced work under:

<https://creativecommons.org/licenses/by-sa/3.0/>



9 783746 066684

List of more than 330 Entries

Introduction

Linda A. Bertram and Gunther van Doobie:

Nomenclatura: What does a modern “Encyclopedia of Cryptography and Internet Security” offer for the education, discussion and sovereignty of learning professionals? - An interdisciplinary view on the Transformation of Cryptography: Fundamental concepts of Encryption, Milestones, Mega-Trends and sustainable Change in regard to Secret Communications and its Ideas, Key-Terms, Definitions and Good Practice.....17

Access Control62	Authorization	79
AE - Adaptive Echo	AutoCrypt	80
AES - Advanced Encryption Standard	Availability	80
AE-Token66	Backdoor	81
Algorithm	Big Seven Study (2016)	84
Alice and Bob	Biometric Passport	85
Android	Birthday Problem	87
Anonymity	Blinding	88
Answer Method70	Block Cipher	90
Asymmetric Calling	Bluetooth	92
Asymmetric Encryption	Botan	92
Attack	Bouncy Castle	93
Audit	Broadcast (in Cryptography)	94
Authentication	Brute-force Attack	94

Bullrun (Decryption Program)	95	Cryptographic Discovery	117
Button	96	Cryptographic DNA	118
Buzz / e*IRC	96	Cryptographic Protocol	119
C/O - (Care-of)- Function	97	Cryptographic Routing	120
CBC - Cipher Block Chaining	97	Cryptographic Torrents	121
Caesar Cipher	98	Cryptography & Cryptology	122
Certificate Authority .	100	CryptoPad	123
Chaos Theory	101	Crypto-Parties	124
Cipher	102	CrypTool	125
Ciphertext	104	CSEK - Customer Supplied Encryption	
Ciphertext Stealing	105	Keys	126
Clientside Encryption .	105	Data Exposure	127
C-Mail	106	Data Obfuscation	127
Collision Attack	106	Data Validation	128
Complexity	106	Database Encryption ..	128
Confidentiality	109	Decentralized Computing	130
Configuration	109	Delta Chat	130
Congestion Control	109	Democratization of Encryption	132
Continuous Improvement	109	Deniable Encryption ...	132
Corrective Action	111	DFA - Differential Fault Analysis	133
Crawler	111	DHT - Distributed Hash Table.....	134
Credential	111		
Cryptanalysis	112		
Crypto-Agility	114		
Cryptogram	114		
Cryptographic Calling	115		

Digest Access Authentication	134	EPKS - Echo Public Key Share Protocol.....	161
Digital Signature	135	ETM - Encrypt-then-MAC.....	162
DNS - Domain Name System	137	Exponential Encryption	164
Documented Information	138	Exponential Key Exchange	166
Dooble Web Browser .	138	E2EE - End-to-End Encryption.....	167
DTLS - Datagram Transport Layer		Facial Recognition System	168
Security	139	Fiasco Keys & Fiasco Forwarding	169
Eavesdropping	139	File-Encryptor	170
ECHELON	141	File-Sharing	170
Echo (Protocol)	143	Fingerprint	171
Echo Accounts	146	FinSpy	172
Echo Match	146	FireChat	173
Echo-Grid	147	Firewall	174
Echo-Network	148	Flooding	175
Edgar Allan Poe	149	Forward Secrecy	175
E-Government	150	Forward-Secrecy-Calling	176
ElGamal	152	Freedom of Speech	176
Elliptic-Curve Cryptography	152	Freenet	179
E-Mail Institution	154	Full Echo	179
Encapsulation	154	F2F - Friend-to-Friend	179
Encryption	155	GCM - Galois/Counter Mode-Algorithm	180
Enigma Machine	155	Gemini	180
Entropy	159		
Ephemeral & Session Keys	159		

GnuPG - GNU Privacy Guard	182	Information-theoretic Security	199
Gnutella	182	Information Theory	199
Going the Extra Mile ...	182	Innovation	202
Goldbug (E-Mail Password)	184	Instant Messaging	203
GoldBug (Software)	184	Institution	204
Goppa Code	185	Integer Factorization	205
Graph-Theory	186	Integrity	206
Group Chat	188	Internet	207
GUI - Graphical User Interface	189	Internet Security	207
Half Echo	189	IPFS - Instant Perfect Forward Secrecy.....	208
Hash Function	190	IRC – Internet Relay Chat	209
HMAC - Keyed-Hash Message		Isomorphism	209
Authentication Code..	191	Iterated Function	210
Homomorphic Encryption	192	Java	210
Homomorphic Secret Sharing	193	Juggerknots / Juggerknot Keys	211
HTTPS	193	Juggernaut PAKE Protocol	212
Human Rights	193	KDF - Key Derivation Function	214
Hybrid Encryption	196	Kerberos	215
Identification	197	Kerckhoffs' Principle	216
IMAP - Internet Message Access Protocol	197	Kernel	216
Impersonator	197	Key	217
Information Security ..	198	Keyboard	218
		Key Exchange / Establishment	218
		Key Size	223

Key Stretching	224	Monitoring	247
Keystroke Logging	226	Moore's Law	248
KeySync	227	Mosaic	248
Lattice-based Cryptography	227	Multi-Encryption	249
Libcurl	229	Mutual Authentication	250
Libgcrypt	229	Neighbor	251
LibSpotOn	229	Netcat	251
Listener	230	Neuland	251
Login	230	NIST - National Institute of Standards and Technology	251
MAC - Message Authentication Code ..	230	NOVA	252
Magnet-URI	231	NTL - Number Theory Library	252
Malleability	232	NTRU	252
Mass Surveillance	233	Null Cipher	253
Matrix	236	Number Theory	254
Matryoshka Doll	237	OFFSystem	255
McEliece Algorithm	239	OMEMO	255
McNoodle Library	240	Open Source	256
Measurement	240	OpenPGP - Open Pretty Good Privacy ...	256
Media Bias	240	OpenSSH - Open Secure Shell	257
MELODICA - Multi Encrypted Long Distance Calling	241	OpenSSL - Open Secure Sockets Layer ..	257
Mesh Networking	242	Opportunistic Encryption	258
Meta-Data	244	OTM - One-Time-Magnet	259
MITM – [Hu]Man-in-the-middle Attack	244		
MITM - Meet-in-the-middle Attack	246		
Mix Network	247		

OTP - One-Time-Pad	259	Private Key	280
OTR - Off-the-Record	260	Private Servers	281
Ozone Address		Pseudorandom	
Postbox	260	Number Generator	281
Padding	261	Public Key Certificate	282
Pandamonium	262	Public Key	
Passphrase	263	Cryptography	283
Pass-through	263	PURE-FS - Pure	
Password	264	Forward Secrecy	284
Patch-Points	264	P2P - Peer-to-Peer	284
Pegasus Spyware	264	Qt	284
Pepper	265	Quantum Computing	285
Performance	266	Quantum	
PGP	266	Cryptography	285
Pigeonhole Principle ..	267	Quantum Information	
PKI - Public Key		Science	287
Infrastructure.....	268	Quantum Logic Gate	288
Plaintext	269	Rainbow Table	288
Plausible Deniability ..	270	Random	289
Point-to-Point	271	Random Number	
Policy	272	Generation	289
POP3 - Post Office		Raspberry Pi	292
Protocol	272	Remote Control	
POPTASTIC	273	Systems Spyware	292
PostgreSQL	274	REPLEO	293
Post-Quantum		Replay Attack	293
Cryptography	275	Requirement	294
PRISM (Surveillance		RetroShare	294
Program)	276	Review	295
Privacy	277	Rewind	295
Privacy Amplification	279	Rosetta-CryptoPad	295

ROT13	297	Smoke Crypto Chat	
Routing	298	App	316
RSA	299	SmokeStack	317
Salt, cryptographic	299	SMTPS - Simple Mail Transfer Protocol	
SCTP - Stream Control Transmission		Secured	317
Protocol	300	SMP - Socialist Millionaire Protocol ...	317
SECRED - Sprinkling Effect.....	300	SMP-Calling	319
Secret Streams	300	Splitted Secret	319
Secure by Design	301	Spot-On Encryption Suite	321
Secure Channel	301	SQLite	321
Secure Communication	303	StarBeam (Ultra- StarBeam)	322
Security	304	StarBeam-Analyser	322
Security through Obscurity	304	Steganography	322
Selectors	305	Stream Cipher	323
Server	308	Super-Echo	325
Session Management .	308	Surveillance	326
SHA-3	309	Surveillance, global	328
Shared Secret	310	Symmetric Calling	330
Shor's Algorithm	310	Symmetric Encryption	330
Side-Channel Attack ..	311	Symmetric Key	331
Signal Protocol	312	TCP - Transmission Control Protocol.....	331
Simulacra	313	The Ali Baba Cave	331
SIP-Hash	314	The Bombe	335
Small World Phenomenon	314	ThreeFish	336
Smoke Aliases for Key Exchange	316	Timing	337

TLS - Transport Layer Security	337	URN - Uniform Resource Name	354
Token	338	Vapor Protocol	354
Tor	340	Virtual Keyboard	355
Tracking Cookie	340	VEMI - Virtual E-Mail	
Triad of CIA	342	Institution.....	356
Triple DES	345	Vigenère Cipher	356
Trojan Horse	346	Volatile Encryption	359
TEE - Trusted Execution Environment	347	Web-of-Trust	359
Turing Machine	348	Wide Lanes	360
Turtle-Hopping	350	XKeyscore (Surveillance Program)	360
Twofish	351	XMPP - Extensible Messaging and Presence Protocol	361
Two-Way-Calling	352	XOR	361
UDP - User Datagram Protocol	352	YaCy	362
URL - Uniform Resource Locator	353	Zero-Knowledge-Proof	363
URL-Distiller	353		
RnD-Questions	364		
Index of Figures	368		
Bibliography	372		
Index of Keywords	397		

Applied Instructions of Thessalonicher

Now we ask you, sisters and brothers, to acknowledge those who are working among you, who care for you and who admonish you. Hold them in the highest regard in love because of their work.

*Don't spit into the soup of others,
if not able to provide excellent alternatives.
Live in peace with each other.*

And our desire is that you, sisters and brothers, warn those whose lives are not well ordered, encourage the disheartened, help the weak, be patient with everyone.

Make sure that nobody pays back wrong for wrong, but always strive to do what is good for each other and for everyone else.

*Have joy at all times, stay curious,
invent and create continually,
give thanks in all circumstances;*

Do not put out the light of the Spirit;

Do not treat prophecies with contempt.

*Instead: Test them all and hold on to what is good
(for yourself, me and all of us).*

Introduction

Nomenclatura: What does a modern “Encyclopedia of Cryptography and Internet Security” offer for the education, discussion and sovereignty of learning professionals?

- An interdisciplinary view on the Transformation of Cryptography: Fundamental concepts of Encryption, Milestones, Mega-Trends and sustainable Change in regard to Secret Communications and its Ideas, Key-Terms, Definitions and Good Practice.

by Linda A. Bertram and Gunther van Dooble

Until now, the creation, application, and research of cryptography and its algorithms and processes as well as the programming of corresponding software were reserved for state institutions, subject matter experts, and the military.

In the recent past, in addition to the centuries-old encryption with a secret key, the encryption with a key pair - consisting of a public and a private key - has been established.

In this case, by means of mathematical calculation (a prime factor decomposition) with the public key of the communication partner and the own keys, a message can be correspondingly encrypted and decrypted again.

It is an encryption not with a shared secret, but with a so-called "Public Key Infrastructure (PKI)"(↗): Just the pair of

keys, one of which can be public - and the other, which is private.

Since then, these two methods of encryption exist: The method of using a secret key is known as symmetric encryption (↗) (both communication partners must know the password) and PKI encryption with a public and a private key is known as asymmetric encryption (↗).

The description of the transmission of a symmetric credential in asymmetric encryption - without any major security concerns - was a milestone in cryptography.

Since then, modern cryptography has evolved steadily. Today, mathematical knowledge has greatly expanded with respect to the field of cryptography. Process-oriented, breathtaking concepts and inventions that have brought the protection of texts – our written communication – further forward and made it safer have also been discovered.

In the following, we want to highlight and summarize more than two dozen fundamental concepts, milestones, megatrends, and sustainable changes to secure online communication and encryption that also provide a foundation for the need to publish a modern encyclopedia.

The heyday of "end-to-end encryption" (1)

The conversion to respective supplementation of point-to-point encryption with end-to-end encryption (↗) has not only been carried out technically, but also in common language use: both encryption routes (point-to-point as well as end-to-end) have been present structurally, however, the awareness of end-to-end encryption has

become increasingly important as Internet and mobile communications began to become more and more intercepted at the beginning of the 21st century.

Everyone today speaks of end-to-end encryption. Yes, "end-to-end encryption" is even used by many citizens as a term for "encryption" itself. We ask ourselves today if the connection between you and I is also completely encrypted, that is, completely encrypted from my end to your end, and thus without any gaps.

Because, a point-to-point encryption in e-mail and chat – such as with the well-known XMPP-chat (↗) - means that the user to the server has transport encryption. The server can read the data, and then encrypt it before sending it again point-to-point (transport) encrypted.

This also shows that legacy chat protocols or transport encryption were designed at the time and that the corresponding applications today have architectural problems due to the lack of programming of (continuous) end-to-end encryption - or at least make efforts to fill these gaps.

End-to-end encryption often needs to be requested or prescribed and installed later.

For example, XMPP has released a manifest for encryption (Saint-Andre 2016), but only a few clients and servers have improved their content and code so far.

There remain questions about a fragmented IT architecture as well as questions about the content quality standard: whether all modern possibilities can be elaborated in the lowest common denominator.

That means that the newer developments - firstly to equip the clients based on the algorithm RSA (↗) with alternative

algorithms such as NTRU (↗) and McEliece (↗), and secondly the option of a quick and frequent exchange of end-to-end keys - were postponed into one by the manifest undefined future.

In an IT landscape of numerous clients and servers, this requires considerable programming effort or, consequently, the exclusion of plain text on each forwarding server: If you wanted to disable all XMPP messengers with RSA encryption, and you would want to ban all servers to forward plaintexts - so they follow the end-to-end paradigm consistently - XMPP would be in a desolate state, as the infrastructure often could not achieve this quality and security status.

The manifesto remained gentle and predicted little: "This commitment to encrypted connections is only the first step ... and does not obviate the need for technologies supporting end-to-end encryption (such as Off-the-Record Messaging or OTR(↗)), strong authentication, channel binding, secure DNS, server identity checking, and secure service delegation" (*ibid*).

To „not obviate supporting end-to-end encryption in XMPP“, does not mean to make it good practice or even mandatory.

XMPP thus remains - despite the pleasant standardization in the area - in terms of encryption, a dinosaur, which is best corrected for security reasons, because the common or even modern standard in terms of cryptographic processes is not achieved here.

Anyone who has grown up with plaintext-XMPP will possibly defend the well-known with high emotions and the cryptographical development - for example, that today is

referred to further developed end-to-end encryption - becomes a crypto-war, if not a religious community-war, that ignites on developers, who have not yet been able to code-out the plaintext capabilities of servers.

For example, in his FOSS-ASIA presentation in 2018, Daniel Gultsch lists 8 out of 30 popular XMPP servers without XEP-0384 OMEMO (↗) encryption with the comment: “The problem of the fragmented Ecosystem XMPP is that it has outdated servers, which don't support those latest encrypting extensions. Part of the Solution is to make the problem visible” (2018-08:55).

The conversion of this architecture and infrastructure to native and end-to-end encryption is not yet, at least years after the encryption manifest, in the best garb of good practice, as it was the case with the more promising XMPP-servers Prosody and Ejabberd.

However, the evolution of end-to-end encryption in other messengers and in IT in general now clearly shows that the paradigm of end-to-end encryption has become a predicate value, which sets secure encryption - without a third party reading in the middle - as a standard.

If a (at that time) de facto communication standard such as XMPP calls all - servers, as well as clients, e.g. to implement higher standards or even end-to-end encryption, and the implementation is still not sustainable, at least as long there is room for further activities and instances without encryption are not turned off, this shows not only the fragmented state with respect to antiquated standards, but at the same time a heyday of end-to-end encryption, which is on everyone's agenda today.

And thus, old standards with this new standard outdates or stimulates the comprehensive revision with further steps because the end-to-end encryption has evolved itself, as follows:

Manifesting End-to-End Encryption in „Cryptographic Calling“ (2)

In many cases, encryption software has one encryption key per online session. As an example, the OTR encryption (a forerunner of OMEMO encryption) can be considered: Again, one key per session was sent.

However, more advanced programming can now send any number of temporary keys per online session through a secure channel. This is called Cryptographic Calling (↗).

Secure communication with a friend has thus become convenient, as we know from a telephone call: pick up and call the handset, and end the session after or in the middle of a conversation by putting the handset back on its hook. Respectively for the smartphone generation: the conversation is ended with the push of a button. Regardless of the duration of each online session, especially on always-on devices.

Another criteria was that the previous session orientation changed into a generation of end-to-end encryption at any time. Forward Secrecy (↗), meaning the use of temporary end-to-end encrypting keys, went into serial production with key generation. It broke out of congruence with the session.

Instant Perfect Forward Secrecy (IPFS) (3)

Cryptographic Calling meant that a time frame was no longer bound to sessions, but a user could execute a "Cryptographic Call" "at any time" and "immediately" and renew the temporary, end-to-end encrypting keys.

Perfect Forward Secrecy (↗) - that is, protection by temporary keys - has become "instant": security has been implemented for immediate application and renewal, hence the term: Instant Perfect Forward Secrecy (IPFS) (↗).

The Melodica Button (4)

In this context, another term emerged in the application world: The term "Multi-Encrypted-Long-Distance-Calling". Alone in its abbreviation "MELODICA" it is already indicated that with end-to-end encryption should be played nimble and fast, it must be renewable at any time, much like a musician plays the keys on a musical instrument.

MELODICA (↗) was a button that allowed users to automatically renew the end-to-end encryption by pressing a button: The MELODICA button was built into the UI of Crypto Messenger GoldBug (↗) as a graphical element for the Instant Perfect Forward Secrecy (IPFS) process described above and logically the icon represented a piano keyboard with white and black keys.

When pressed, new symmetric keys are transferred for temporary purposes through a permanent secure channel to open a new temporary communication channel. However, the button disappeared with the elaboration of

the various other methodological types of Cryptographic Calling.

Cryptographic Calling was first programmed into the Encryption Suite "Spot-On" (↗) in 2013 and then continuously elaborated and further developed. Today, different methodological types of Cryptographic Calling can be distinguished.

Elaboration of the methodical types of Cryptographic Calling (5)

More important than being able to renew the end-to-end encryption multiple times during a session (making it very difficult for attackers to succeed in attempting to catch or find end-to-end encrypting keys), was the fact that methodically could now be played with the existing hybrid encryption and Multi-Encryption.

The secure channel for transmitting temporary keys could be both symmetrical and asymmetrical.

And now, in the asymmetric channel, either a symmetric key could be used for the temporary forward-secrecy key, or a temporary asymmetric public key could be used.

The same was due of course vice versa for a symmetrically-encrypted channel. And thirdly, the temporary key no longer needs to be sent through the permanent key channel, but can also be sent through a secure channel of an existing (previous) temporary key.

For example: An (asymmetric) temporary key follows a (symmetric) temporary key. With the Spot-On-Encryption Suite, which established the Cryptographic Calling, therefore, at the same time a quasi birth - at least one hour

of enrollment – of the programmed Multi-Encryption (↗) was given:

No other encryption program encrypted messages multiple times at this time and was able to send the new temporary keys so varied and instant.

The various types of Cryptographic Calling (↗) joined the now historic MELODICA button, as there were now more than a handful of possible ways and variants of calling, as the article (↗) entry to this in the encyclopedia further elaborates.

With Cryptographic Calling, (possibly already multiple) encryption received another encryption layer.

Multi-Encryption (6)

Applied programming of hybrid encryption (means in the end that different variants are used at the same time or one after the other) finally led this theoretical and so far little-studied concept of Multi-Encryption with its variety of options into practical application processes.

It is with the Multi-Encryption not only about encrypting a ciphertext again. It's also about possibly changing the algorithm of encryption in the second round.

While an algorithm knows several rounds, operations, repetitions of e.g. substitutions, multi-encryption now puts a whole new dimension on top of it: If Plaintext has been converted to a ciphertext with the RSA algorithm, and this is then converted to another ciphertext by the McEliece algorithm: What comes out at the end? And can this be better or worse analyzed using the usual methods of cryptanalysis (↗)?

It is no longer just a question of substituting individual characters, but a completely new algorithm is applied to the ciphertext end product of a previously used algorithm. Multi-Encryption thus consists of three main areas: The multiple encryption (conversion from ciphertext to ciphertext), and secondly, a mixture of algorithms, to thirdly the mixture of methods; which could certainly also fall under algorithms, therefore we say: Process chains: The mixture also of the transfer ways of the keys, for example, complements methodically and procedurally the mixture of algorithms, because it is a difference whether RSA-AES-McEliece triple changed ciphertext is sent through a channel of a permanent key or is sent through the channel of a temporary key.

Multi-Encryption has become the mega-topic of current cryptography and its analysis through this applied programming and conceptual elaboration; and was named as a research area in many online portals and forums like Reddit and others - more than ever before on the agenda.

Further research will be dedicated to these three aspects of multi-coding, as this new quality may also reveal security gaps or vulnerabilities of certain algorithms.

As an example: Is ciphertext, which has been converted three times with RSA-AES-McEliece, more meaningful in reference to a plain text than a just one-time RSA-only converted plaintext to ciphertext? Or in the comparison of three times with RSA converted plaintext? Respectively is three times RSA-converted text less secure than a three times McEliece-converted text?

Of course, Multi-Encryption is also associated with interests at the owners of existing solutions, definitions and

processes, if the structure could be strengthened or weakened by an algorithm, if ciphertext is again converted to ciphertext by a (further) algorithm.

The applications which up to now use Multi-Encryption assume that the encryption becomes particularly secure if ciphertext is repeated for another conversion to ciphertext, e.g. if it is encrypted symmetrically and then sent through a TLS(↗) channel. For the reverse conversion from ciphertext to ciphertext in several rounds, additional security must therefore be assumed - until dedicated research studies could indicate otherwise. Anything else would be illogical assumptions, because: Double-encrypted is better.

Multi-Encryption requires programming knowledge from mathematicians (7)

Combinatorics can no longer refer to the application of only one procedure from a discipline, but integrates hybrid and multiple up to exponential processes from different disciplines. The practice and theory of encryption is complete, if, in addition to mathematics and combinatorics also applied programming is added, as well as: If network theory, graph theory, and other departments are supplemented.

Cascading and Multiple Encryption is not only a young field of research, but gets and finds significant boost and complementary additions in all these neighboring disciplines. If you want to deal with encryption in the future, at least together with your team one should also be able to program appropriate software for Multi-Encryption and the mathematical algorithms in one of the popular

developer languages: Mathematical calculations have to be supplemented by the knowledge of applied software programming in order to be able to obtain the resulting ciphertext by the computer-aided calculations.

REPLEO (8)

In the centuries-old symmetric encryption with a password or an known algorithm, which reverses the letters or characters, the key may under no circumstances be revealed – also according to the well-known Kerkhoffs's principle (↗) - that states, that not the algorithm should be protected, but in particular the key.

Indeed, Kerkhoffs lived at a time when there was still no asymmetric encryption existing with PKI respectively a private and public key. But what if this principle would be also applied to asymmetric encryption? Anyone here would say that the “public key” does not mean “public key” for nothing? - It can be made public. However, it is though technically possible, as soon as I have received the public key of a friend, to convert my own public key - before sending it - with this, their public key to ciphertext. This is called REPLEO (↗) and protects the public key.

The Kerkhoffs's principle referred to asymmetric encryption - aka titled "Kerkhoffs's principle of asymmetry" - is thus a REPLEO, which also encodes and protects the public key of PKI at a transfer of the key.

But this is not yet a solution to the key transport problem - which is essentially in the symmetric encryption with a passphrase – instead it is only a protection of the public key

of asymmetric encryption, for those who do not want to make this public key public to everyone.

But how can a symmetric key, a secret passphrase, be securely transmitted over the Internet? By sending it over a secure channel. One possible method dedicated to this question was given with a so-called EPKS channel.

The EPKS-Method (9)

Symmetric keys - e.g. a passphrase - can be securely transmitted between two nodes on the Internet using an EPKS-channel (↗). The EPKS-channel allows to send the key over this channel. And channel message recipients have then automatically integrated the key into their instance, and could use this key to further decode messages.

The EPKS-channel was first integrated also in the above-mentioned Encryption Suite, as it was one of the early comprehensive software that sent keys through encrypted channels, which in turn could be then used as an own encrypted channel.

It is implemented there in such a way for any content or purpose, however, it was integrated for the transmission of URLs or own bookmarks from a URL database to a friend or circle of friends as a default template (URL Community).

The automated transmission and integration of keys over the EPKS-channel was presented as a model of secure key transmission with this concept capture and programming within the so-called Echo Protocol (↗): Echo Public Key Sharing (EPKS).

AutoCrypt (10)

In derivative applications, concepts of automated key transfer and key integration of EPKS have been deduced, e.g. also integrated under the name AutoCrypt (↗) in various e-mail and chat applications. At the beginning, two e-mail users exchange an e-mail that ensures that both users can swap their public PKI key. If this is the case, the keys are exchanged and all other e-mails are continuously encrypted with the public key.

Reading State-of-the-Art Signals: Fiasco Forwarding with Fiasco Keys (11)

Thus, when a subscriber resends with old traditional messengers after a received message again for the first time, he / she renews the session key material again by a so-called Diffie-Hellman key exchange (asymmetric key), in which e.g. its own new key is combined with the already-known key of the remote station (D/H-Ratchet).

In this Ratchet method, symmetric keys are derived from the session key material using a key derivation function. Since the key derivation function is based on a hash function, this step is called a hash ratchet. For each message, the protocol relays one of two hash ratchets (one to send, one to receive) initialized based on a shared secret from a D/H-Ratchet.

At the same time, it tries to provide the remote station with a new public DH value at each opportunity and to push on its own local DH ratchet each time a new public DH value arrives from the remote station. This method has

been incorporated in numerous known commercial messengers (such as WhatsApp).

Security experts see weaknesses here, when in commercial or even proprietary products no own server can be used. In addition, the schematic consequence of "pushing on" the keys is considered a special vulnerability: If a key is in a defined location, it is also easy to find.

And: Keys are still being exchanged, which could be derived using a zero-knowledge-proof-method (↗) without exchanging the key.

After all, why not create and send a dozen keys per chat message that are collected in a pool and are all tried out, from the most recent to the oldest, per received message? Or also create (symmetric) keys that are formed according to a two-way calling (↗) by both sides, in which each communication partner contributes 50% in the generation and exchange of the secret, symmetric password in this type of Cryptographic Calling? Fifty-Fifty as a method in the formation of common keys.

This further method of sending numerous keys - besides two-way calling - is called Fiasco Forwarding (↗) with corresponding Fiasco Keys (↗) and was first developed in the Smoke Messenger (↗) as Java code.

Although this messenger is not commercially distributed and therefore less popular, it is on the protocol level, a fuller and more secure security-design than the previous mentioned Signal Protocol for end-to-end encryption with a Ratchet method, which also inserts no manual and individual Cryptographic Calling (end-to-end encryption with user-defined passphrases), do not allow the use of

easy-to-administer own servers and even is not open source when using popular communication servers.

So anyone who turns the Signal (↗) Protocol - as this schematic Ratchet method is now called - in the sense of mobile encryption as state of the art, is no longer up to date: The extremely volatile design using Fiasco keys or a Fiasco Forwarding has significant advantages over other, more schematic protocol implementations.

With these innovations - REPLO such as EPKS or the derivative AutoCrypsts - on issues of the key transport problem, the key transmission is only better protected with a further layer of security respectively (at AutoCrypt) more convenient for the user only through automated key acceptance.

However, Fiasco Forwarding with its Fiasco Keys multiplies the number of keys in advance and further develops schematic procedures with so far only one key per message, so that one can speak of a Volatile Encryption (↗).

Volatile does not mean that encryption is shaky and uncertain, but volatile encryption refers to unsteady and temporary keys that are fluctuating, volatile, and evaporating - thus reducing the chance of decryption by multiplying the amount of decryption attempts required per message.

A fundamental innovation in terms of key transmission and risks is the innovation of the Secret Streams and Juggerknot Keys. The key is no longer transmitted via the Internet, but mathematically and methodically formed and derived on each side.

The third Epoch of Cryptography: Solving the key transport problem as another innovative breakthrough in cryptography? (12)

As has been the case, the passing on of a symmetric key - a passphrase - to the communication partner constituted until recently a security-relevant problem and a central aspect of the analysis in order to decrypt cryptography, or to gain insights for it.

Another innovative breakthrough in cryptography was given with another step in the solution of the key transport problem, which was evidenced by the two concepts and programmed procedures "Secret Streams" (↗) and "Juggerknot Keys" (↗).

With that, two communication partners can communicate encrypted with each other via an Internet infrastructure, without having to transfer the current key via the Internet. These potentials offer epochal changes in cryptography.

Because the application of a zero-knowledge proof for the derivation of keys on both sides of the communication partners from a common unspoken level of knowledge, the external is not obvious, is not only mathematically brilliant, but also represents a groundbreaking development in cryptography in this process design when the well-known key transport problem experiences these various innovative solution perspectives.

Let's describe each innovation in this new direction in turn:

Cesura in Cryptography: Secret Streams (13)

Secret Streams denote the creation of numerous temporary keys, that are in the build process derived from a not-over-the-network transmitted passphrase. The keys come or derive out of a Socialist Millionaire Process (SMP) (↗).

In this process, both friends enter a secret password in their client - and this is not transmitted over the Internet. Using a mathematical method, a zero-knowledge proof, it is determined whether the same password has been entered on both sides.

The so-called Socialist Millionaire Protocol produces the mathematical calculation of this Zero-Knowledge Proof.

The Socialist Millionaire Problem is one in which two millionaires want to determine if their wealth is equal without disclosing any information about their riches to each other. It is a variant of the Millionaire's Problem whereby two millionaires wish to compare their riches to determine who has the most wealth without disclosing any information about their riches to each other.

If the mathematical SMP proof is successful, it can be assumed that both communication participants have entered the same password into the mathematical process in each of their clients - without, however, that this password has ever been transmitted over the Internet.

This method of the Secret Streams, which until now has only been used in two programmings, as well as the Juggerknot Keys(↗) might therefore be regarded as further milestones - if not even as the beginnings of a possible new epoch - in cryptography: While we have just seen above

that end-to-end encryption is currently experiencing its popular heyday, this flowering has long been outdated by this cryptographic design: passwords encrypting end-to-end no longer have to be transmitted over the Internet!

It certainly needs furthermore secure channels, but there is no need to transfer a key online over these channels - as it was the case when sending a symmetric key.

While the PKI as a "new direction" has become modern with the secure transmission of the key in the Diffie-Hellmann exchange, today it is also for the symmetric encryption pointed out that - thanks to this "new direction" Secret Streams - no symmetric key must be transmitted anymore over the network from one end to the other end. Secret Streams can be another big step in cryptography following the invention of asymmetric encryption, solving the key transport problem and eliminating Kerkhoffs' principle.

Thus, Secret Streams could also be discussed as Kerkhoff's Principle Number 2, as a dialectical reference function of Kerkhoff's Principle, or even as Kerkhoff's Inversion.

Of course, both communication partners first have to discuss a common level of knowledge or experience with minimal communication: e.g. in advance in real life.

In the way: Can you still remember the name of the restaurant in which we met? Please enter this name as a phrase in the communication client.

The phrase is not transmitted over the Internet, but the mathematical calculation of the zero-knowledge proof shows us whether we both entered the identical passphrase; and we too are authentic persons. Then

numerous temporary keys are derived identically on each side by the method / function of the Secret Streams.

Secret Streams are programmed in C ++ and were first developed in the popular and already named Encryption Suite Spot-On.

They offer potential to dispense with the transmission of keys in secure and unsecured channels of the Internet.

Cesura in Cryptography: Juggerknot Keys (14)

An elimination of the key transport problem is also found in the Juggerknot Keys. These are exemplary programmed in Java (in the application of the Crypto Chat Messenger Smoke (↗) for the Android operating system) and build on a similar method of a Zero-Knowledge Proof: With the difference that here not a (Socialist-Millionaire) SMP process was used, but the mathematically-similar process of the Juggernaut PAKE Protocols (↗), in which both communication partners - each on the own side - also enter a secret phrase, which in turn is again not shared over the Internet. Then, temporary end-to-end encrypting keys are derived.

Also here it can be spoken not only of a mathematically-stunning process, but also of an innovation in cryptography: Encryption without a critical transfer of the key over the Internet.

After symmetric encryption, the establishment of asymmetric encryption and now the solution of the key transport problem with zero-knowledge proofs with derivative keys, this third epoch of cryptography is not only a new descriptor for theoretical cryptography, but also a

model for programmers in their applied development, since the open source programming in both major programming languages (C++ and Java) are available as software libraries. Now you might want to consider that you have to exchange a secret before using the online Internet infrastructure, so this is only partially correct, because it is about picking up a keyword from a common pool of experience, without naming this keyword. Ultimately, in the simple case, each communication partner is indexed or mapped only once with an alias, and henceforth, encryption can take place without the transfer of keys over the Internet - each with freshly derived keys.

So, if the British agent knows that he has to mentally map his friend, the American agent, with the password "Houston," and the Russian agents with the password "Moscow" and the Chinese agents with the password "Beijing," then they need in the third epoch of cryptography no key exchange anymore, but only a messenger and appropriate network or Internet architecture (i.e. an online connection) to communicate undisturbed. When the British agent talks to the American agent, they both enter the phrase "Houston".

Transferring current (fresh) keys over the Internet is no longer necessary; they are derived from the remembered agreement of both communication partners, which only need to be agreed once and then mathematically proved – that means at the same time, the communication partner is also authenticated - but can henceforth communicate under the paradigm of "Instant Perfect Forward Secrecy" (IPFS).

The solution of the key transport system by means of Secret Streams and Juggerknot Keys, in which the symmetric key on both sides are formed by a mathematical zero-knowledge process and therefore no longer have to be transmitted over one channel, defines a new perspective for programming and the further future in cryptography.

Machine learning using cryptographic tokens - using the example of the Adaptive Echo (15)

Using cryptographic tokens not only machines in the network can be controlled, but also paths can be defined according to a graph design in the network. As an example, the elaboration of the Adaptive Echo (↗) may be mentioned, in which a connected node excludes by means of a cryptographic token that another connected node receives a certain information.

The uninformed node does not even know that its connected network environment is denying it a particular message.

This would be comparable to a historical example in the analogue world, as if in August 1941 Admiral Kimmel had been deprived of "Security Reasons" (Possony 2013: 204) as well as Pearl Harbor itself highly significant news related to the port and the fleet, and the Japanese apparently did not send the messages - or at that time the decoding codes - anymore.

In today's digital network, machines and nodes therefore learn when they receive information, or else they receive

no information. Adaptive protocols are therefore to be combined with an Environmental Learning.

"Machine Learning" has become "Environmental Learning" because the context of all machines in the network has to be considered when neighbor machines learn by not including their own machine in the learning process of others.

Adaptive protocols such as the aforementioned AE Protocol give us the opportunity to modernize and refine the terms and content - as it is comparable the case with: "good practice" rather than "best practice" and "extra-occupational learning" rather than "lifelong learning", or "Work-Life-Learn-Balance" instead of "Work-Life-Balance". And here: "Environmental Learning" instead of "Machine Learning".

It would still be comparable if this encyclopedia is exchanged as a book among the learners, but the teacher is not informed. With the question or suggestion of a pupil in class as to whether the practice of a "cryptographic cafeteria" can be provided in the classroom (as further explained in detail at the end of this paper), it would be possible for the student to determine with the teacher's answer whether the teacher would be an included or exempted "network node" with knowledge of this lexicon.

While the Borg collective known from the Star Trek films assimilates and alters new entities, environmental learning deals with exactly the reverse process: extracting a node from the flow of information, so that other machines have a knowledge leap or information advantage, and learn accordingly and the assignment of rights for a neighbor machine is defined. Thus, by means of Cryptographic

Tokens (↗) and adaptive protocols (such as the AE protocol), a machine – and also often human beings – can only collect the information that is also made available to them.

This leads to the process of Cryptographic Discovery (↗). These are "discovery processes" that use cryptographic values in a network landscape. Machine Learning has expanded into Environmental Learning and will then merge into an encrypted environment in the concept of Cryptographic Discovery:

Cryptographic Discovery (16)

The concept of Cryptographic Discovery can be understood in the sense of a Distributed Hash Table (DHT)(↗), which further develops it.

A DHT is a data structure that can be used, for example, to record the location of a file in a P2P system. The data is distributed as evenly as possible over all existing storage nodes. Each storage node corresponds to an entry in the hash table. The self-organizing data structure can thus map the failure, accession and exit of nodes. However, this carries security risks: each node knows the address and memory content of all other nodes.

In the concept of Cryptographic Discovery information is now passed on the basis of cryptographic tokens, so that a server can collect information about its environment, in particular via a graph to be controlled to reach the destination, without having to directly index or know the target itself.

For example, if a server receives the information that Alice can be reached through Bob, it does not have to send information to Alice over the route of Ed or Maria. This concept is based on Machine Learning - or, as we have learned, better: Environmental Learning - through cryptographic tokens, as found, for example, in said adaptive protocol. Cryptographic Discovery will therefore need further research in this regard. This concept paper of the communication server SmokeStack (↗) was also used there for pre-programmed processing, which has to be taken up further in terms of information-theoretical analysis as well as with regard to analysis of the program code as a research topic.

This process was bundled in the neatly-worded "Beyond Cryptographic Routing"(↗). It is no longer just about replacing the IP address with a cryptographic value that has been formed, be it through a cryptographic hash function or through a public cryptographic key. But it is about that routing in a "flooding network" or better: "mesh network"(↗) is basically target-less, so we can no longer speak of routing. The "New Direction" is: Some also have "No Direction". Complex chaos. Therefore "Beyond Routing". This has become analyzable and describable from the Echo Protocol (↗) published since the first decade of the 21st century.

Beyond Cryptographic Routing: The Echo Protocol (17)

The Echo is a protocol that has been established for many years and is implemented in various applications as well as

servers for encryption and network design. It creates a flooding or mesh network with its basic rule that the encrypted packets are forwarded to all connected nodes. As with an acoustic echo, all can hear the echo after sending the signal.

It can also be compared to dolphin communication: each dolphin sends out a signal to be picked up and processed by any dolphins surrounding it. Each node that is connected, or any dolphin that can receive the signal or message packet, will process it.

Each node is also a simple reflector in the echo protocol, because every packet that comes in is also sent out again.

Finally, every sent packet in the Echo protocol is always encrypted. And: It can also be Multi-Encryption. Not only is the flooding character free from data retention analysis (with their meta-data to: Who sends when to whom?), But because it carries the character of "Beyond Cryptographic Routing", there is in the analysis no destination address assignable.

Encryption occurs at three possible levels: First, the encrypted packet is secured with asymmetric encryption, that means the public key of the communication partner is used. Furthermore, the message itself can be e.g. encrypted by means of the Cryptographic Calling symmetric (with a passphrase) and thirdly, this packet is sent through an SSL/TLS-secured (self-signed) channel to the communication partner.

These potentials, which develop when Multi-Encryption and Graph Theory combine, offer a whole new paradigm and high-quality, further research content with this now in numerous clients such as Spot-On, GoldBug, FireFlo,

Smoke Messenger, and Smokestack Server Software built-in and well-documented encryption protocol.

In addition to the three layers of encryption and the two basic features of the protocol (fundamental encryption and fundamental shipping to all connected neighbors), a third and further feature of the Echo protocol is an independent innovation and a milestone in cryptography: The characteristics of the Echo-Matches. Because this increases the security of encrypted communication in networks centrally. So why is the echo destination-free and sender-free and therefore particularly secure?

The Echo-Match (18)

The Echo-Match (↗) is the core idea of the Echo: The plaintext of the message is hashed and the hash is appended to the ciphertext as encrypted capsule.

If a recipient with the stored keys of their friends can reconvert the ciphertext to plaintext, and the hash of the ciphertext matches the supplied hash, the message has been successfully decoded with this right key and will be delivered.

Since the hash of the ciphertext message is not invertible and there is no information about the plaintext, it can be safely enclosed. The hash comparisons before decryption attempts of the encrypted echo capsule are then called an Echo-Match.

A successful Echo-Match decides whether the message is displayed in its own client.

The echo match is designed by the supplemental Vapor Protocol (↗) to follow the logic of the TCP protocol (↗),

that means, if an encrypted capsule in a node has been successfully read, a message is returned to the sender again as an acknowledgment.

This can be used to replace the TCP protocol with the Vapor protocol based on the Echo and the Echo-Match, when it comes to creating a completely encrypted network communication, which nevertheless takes place destination-and-sender-free and due to the match-check remains sovereign on your own machine in localhost.

Exponential Encryption: The amalgamation of graph theory with encryption (19)

Combining the just-presented way of multiple encryption with the graph theory, derives from the principle of the Echo Protocol (that each encrypted message is to be sent to all connected nodes) - a multiplying, even Exponential Encryption (\nearrow) (Gasakis/Schmidt 2018).

It is reminiscent of the historical example of rice grains on a chess board field that doubles with every other field on the chessboard. So-called Congestion Control (\nearrow) filters out once processed messages in a node again and relieves the CPU, if a message has already been forwarded and should be forwarded on the chaotic use of the graphs to a node a second time.

The POPTASTIC-Protocol: Chat over E-Mail (20)

Encrypted messages have harmonized e-mails and chats in the common term Messages. Why should you look at e-

mails and chats differently? So on the technical level logically with the POPTASTIC protocol chat also over E-Mail servers like POP3 and IMAP was made possible.

This has been published in 2014 in the Spot-On Kernel as a concept and as programmed code in the messengers Spot-On as well as the GoldBug Messenger.

It was not only described in detail in the project documentation, but also analyzed in detail in the Big Seven study by auditors (2016, 1). Since then, numerous mobile clients such as Delta Chat (1), Ox Talk, Lettera, and Spike have used and developed the POPTASTIC protocol for encrypted chat over email servers in addition to GoldBug and Spot-On.

Since email servers are available everywhere as an infrastructure, the POPTASTIC chat over email has also solved the server issue in communications applications and put them on a broad footing. This not only offers maximum potential in terms of availability, but also in terms of technical-content for further designs as follows:

FileSharing & Turtle Hopping over POPTASTIC (21)

FileSharing must also be encrypted nowadays. Due to the concern about the sharing of copyrighted content, no peer-to-peer networks can be made (if the peer would be an attacker), but must be encrypted done as friend-to-friend (1) in the sense of a web-of-trust (1). This is always available via the infrastructure of a POPASTIC protocol! Now, when sharing and searching files over the network is

made by friends of friends, this is based on the idea of the Turtle Hopping Protocol (↗).

In other words, if file sharing with turtle hopping is now implemented on the basis of the POPTASTIC protocol in one of the above-mentioned clients, the concept would have been transferred to mobile devices, just like the desktop application RetroShare (↗) as one of the few encrypting file-sharing applications.

This is an interesting perspective not only in terms of ideological and technical, but also in terms of law, when a turtle hopping is based on the POPTASTIC protocol and realized in a programmed mobile client, as the authors Gasakis / Schmidt first described as a concept "The POPTASTIC Echo Turtle" (2018: 67).

It projects the existing Web-of-Trust application RetroShare for the desktop only mobile and via given e-mail servers. Because of encryption and available e-mail servers, such programming offers potential to become the new distributed computing model of F2F Crypto-Torrents (↗) in a distributed system or network.

Establishment of sovereign concepts (22)

Another trend has been the possibility of having own public asymmetric keys with external providers e.g. a cloud (Customer Supplied Encryption Keys, CSEK (↗)) or end-to-end encryption with own passwords (Geminis (↗)) on both sides. Users can define their own compositions in terms of values for a Crypto-DNA (↗) or for a key-generation in modern software.

The Age of Quantum Computers: A New Life Cycle with the McEliece Algorithm and the McNoodle Library (23)

On the one hand we have to change the pure mathematical calculation from the insecure algorithms to the safe algorithms for the age of quantum computing.

A prominent example is the product lifecycle of the RSA algorithm, which is gradually reaching retirement age, and with new algorithms such as McEliece and NTRU is considering adding not only a supplement, but also a necessary replacement of itself: Since the algorithm RSA is now considered to be insecure after official announcement by the American Institute NIST ([↗](#)) in 2016 (NIST 2016), because the underlying mathematical method of prime factor decomposition can be broken by fast quantum computers, other algorithms such as NTRU or McEliece need to be used.

The NIST writes: „RSA Public key Signatures, key establishment: No longer secure. ECDSA, ECDH (Elliptic Curve Cryptography) Public key Signatures, key exchange: No longer secure. DSA (Finite Field Cryptography) Public key Signatures, key exchange: No longer secure“ (2016: table 1, page 2).

Mathematical safeguards against the attacks of quantum computers, as well as programming of software that can do this, as well as the special need for secure online communication on the Internet today, require a fundamentally different view on encryption algorithms than they did in the nineteenth century or even at the beginning of the twentieth century.

The approaching end of the life cycle of the RSA algorithm therefore requires programming alternatives into existing software products to save the patient "PKI" from death by transplantation. Or, concretely, to save the XMPP clients with RSA from decay.

Programs that exclusively offer the RSA algorithm have now reached the end of the product life cycle and should no longer be used!

At the same time, there are already very elaborate code and programming bases both within the applications and as a library, both in Java programming (e.g., Smoke Android Mobile Messenger) and in the C ++ programming language (e.g., Spot-On Encryption Suite) - and open source.

Another example is the library McNoodle (↗), which provides the algorithm McEliece open source for C ++ and in Smoke Messenger the code in the Java language.

Source-open implementations of the McEliece algorithm in Java and C++ messenger applications therefore served as model projects, which were to be taken up in research and teaching and are also described here as early indicators of a Transformation of Cryptography.

Cryptography on mobile devices (24)

Finally, the cryptography in the Internet age has changed dramatically with mobile devices: the smartphone seems to be stuck in the purse or in the pocket of each jeans - at least on the way out of the house. Computers in everyone's pocket now encrypt our online communications over the network.

Only a few technologies (such as the car, a heater, or the television) have reached the population just as comprehensively as the Internet and the smartphone. In both areas, privacy and, hence, the foundations of Human Rights (↗) are protected by technical encryption (and not by a written policy in addition): Encrypting technology should now be created especially on the mobile smartphones.

Effects of cryptographic developments on education policy and its nomenclatura

As in every subject area, there is also a vocabulary of technical terms in cryptography.

These more than two dozen groundbreaking developments and innovations are each worth a detailed study on their own - hence this in combination: What a necessary impulse to adapt the conceptual world to modern times and to further deepen, compare, and network it with extensive research.

Further examples of an urgent need to update the nomenclatura are, for example, technical research results or new standards agreed in committees: For example, TwoFish has become ThreeFish(↗), instead of SSL we now speak of TLS (↗) in new versions or SHA-1 has become SHA-3 (↗) converted.

Information sent over the Internet is largely protected by encryption; because they are increasingly also consciously collected by third parties for evaluations, or even tapped, in order to crack them or to tap them by appropriate

techniques or in processes with gaps. Here it is important to exclude security gaps by outdated standards.

In addition to the numerous proprietary applications and applications before 2010, elaborate messaging projects such as RetroShare, Spot-On and GoldBug as well as various mobile device messengers such as Conversations, Delta Chat or Smoke Chat and others (see also the Messenger Scorecards in: Big Seven Study 2016: 32 as well as Edwards 2018: 100) democratizes the encryption of the mobile and online communication of citizens with its open source code. But already two decades after the introduction of the Internet, or a decade after the introduction of the smartphone and the establishment of the currently dominant mobile operating system Android and the corresponding developments of technological protection of content and the communication of computers and mobile devices via the Internet may be due to the rapid development in the IT sector also the half-life of knowledge in the field of cryptography might already be more than 50 percent: It is therefore not wrong to learn, renew, and continuously update this knowledge.

The described developments, innovations, and new applications in cryptography not only influence programming, the professional world with its business processes or an open source community, but in particular the shifting educational processes have to keep pace with this development and Transformation of Cryptography.

Common sense, even with overviews and introductory works from juxtaposed individual perspectives of different authors, can thus change over the years and leads to the necessity of new compilations and article contributions.

Extensive education and training processes in the field of modern cryptography and Internet security with the inclusion of neighboring disciplines are more important than ever today. Thus, this discipline is interdisciplinary and requires an interdisciplinary discourse.

All of this has motivated us to present a modern encyclopedia that seeks not only to provide a modern overview, but also to provide an opportunity to further deepen individual themes and to put the relevant terms together within a framework that will educate learners of how many years enabling professional readers to get an overview of the full picture of cryptography and online security today, and to turn the learner into a speaker describing the described Transformation of Cryptography.

Learning vocabulary seems to be particularly necessary in this particular field of cryptography, because research and academic teaching, with many vocabulary and terms, often involves foreign words - possibly due to the context of the subject area - and emphasizes a rich subject approach.

Nomenclatura - at the same time the title of the present encyclopedia - is the Latin term, which means a collection of (technical) terms.

At the same time, this word is also written with k: Nomenklatura - and refers to the professional departments and the persons who occupy these: In the socialist state of the GDR. There, it was important for networking in society to list and know these professional functions, so that they could also be aspired to by the next generation.

In the same sense of the collection of professional essences, a list of specialized vocabulary can also create the

quintessential ideal dialogue between young talent, established multipliers, and professional experts.

With learned nomenclatura, the offspring will have the competence to involve professional officials in the dialogue and to meet them at eye level.

What a momentum for the development of the subject areas, if - as it was often described in the philosophy - the pupil can report new things to their teacher or even surpasses them with research and learning successes. Leonardo da Vinci is credited with the quote: "Poor the pupil who does not surpass his teacher".

Because, as described above, the theoretical and applied field of cryptography and online security today, due to its transformation, offers more than ever to many recent developments and updates that are addressed by the contents of this book.

To conclude this article, let us take three innovative processes and developments in the field of encryption in an exemplary summary once again with regard to the future design of curricula: Basic concepts such as secure end-to-end encryption, or even the deniability of keys in forward secrecy, have now been extended by new concepts and process innovations. A user today can not only use a session-based key, but also renew it with Cryptographic Calling at any time using different methods of "Cryptographic Calling" for secure end-to-end encryption: IPFS - Instant Perfect Forward Secrecy.

Fiasco Forwarding sends a dozen keys for decoding a chat message in the sense of a volatile encryption.

Even more: Machines and network nodes learn adaptively through the "Cryptographic Discovery"; new protocols

(such as the POPTASTIC protocol, the Echo Protocol or the Vapor Protocol) and cryptographic matching develop a new understanding of routing: Namely, a "Beyond Cryptographic Routing" also in the context of network and graph theory.

So routing is no longer cryptographic routing, but routing has emancipated itself and quasi abolished itself to a state of "Beyond Cryptographic Routing": If the graph theory and network theory is added to cryptography, it can be found in Mesh- and Flooding-Networks such as an Echo Network and Exponential Encryption.

Open Source libraries, such as the McNoodle library for the McEliece algorithm, democratizes encryption even in the age of (post-) quantum cryptography and replaces the RSA algorithm.

The specialist area and faculty is therefore (in) a major transformation: Not only algorithms are dying, but also new developments, processes and innovations are shaping new paths and applications.

As the years go by, new curricula and learning requirements will arise that will not only require a trainer who has gone through such a school to perform, for example, a mathematical calculation, but possibly also to create a programming or application in a self-programmed application, up to network administrations for an appropriate server-client infrastructure.

All this will require not only a strengthening of interdisciplinary centers, but also regional global networks - both in the personal and in the networking of software and departments over the Internet.

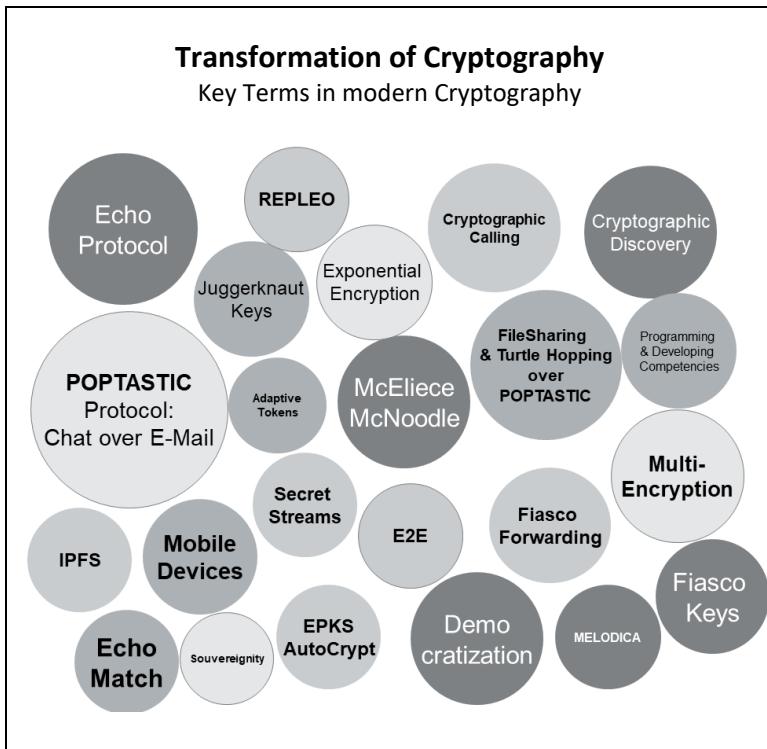


Figure 1: Transformation of Cryptography - Key-terms in modern Cryptography

In order to stem this in the future, to integrate these transformations and interdisciplinary concepts into our educational processes, it requires as an initial start a greater awareness of the current nomenclatura and a learning of the basic vocabulary and facts in cryptography and related disciplines.

So far, however, many of these subjects are in the education of many still a niche and special discipline, which is reserved in mathematics or in learning an applied

programming. There are numerous contents that are worth knowing and also fascinating and can be fun.

The goal must therefore be to transfer the expert knowledge on cryptography into broader general knowledge. This begins with getting to know individual vocabulary, their definitions as well as content and processes.

An encyclopedia that explains these central contents comprehensibly in a broadband overview must therefore be continuously updated or redefined.

In addition to the learners, teachers and multipliers also play a decisive role in the transfer of knowledge.

Therefore, the following exercise should be documented, which can give suggestions for a design of lessons.

The Cryptographic Cafeteria A didactic game for teaching

In preliminary discussions to the publication of this lexicon came in a tutorial on the part of the students the idea and feedback that the topic to learners for a presentation should be chosen by naming a number of 1-300 by the learner.

With this page number, this publication can thus be used to assign a lecture topic to a quasi-random (and therefore also didactically challenging) topic - namely, using the keyword that follows next on the page mentioned.

This educational didactic exercise for the lesson we call "Crypto-Cafeteria" will be designed as a university (and depending on the design also academic) discussion and presentation course and within the 12 sessions of the course the topics randomly from a lexicon curriculum to have chosen, has charm.

As in a cafeteria, the page number of this book allows the learner to choose a "snack", "eat" content, and report to their peers.

In particular with the rule: A learner may skip a keyword found to the next keyword, if they find a partner in the class who jumps back a keyword and selects the previous keyword. The teacher defines the algorithm of how many keywords should jump forward or backward.

As well as: Two students with consecutive pages, may decide independently to work together only one of the two topics found. Furthermore: If you do not want to give a presentation, you should provide a paper with 10-15 pages afterwards.

This "Balance of Karma in Class" rule should certainly promote team development and joint presentations: particularly content-laden topics should be in a team explored, researched and compared, combined, summarized and conveyed. - After a selection using the Cryptographic Cafeteria method.

A cafeteria model (also cafeteria system or cafeteria principle) is called a form of a model in companies for compensation and benefits. The intention of this model is to increase motivation through individual and free choice within an available portfolio.

The system is to be assigned to the cognitive theories of choice in the motivation theories. In the company area, depending on the position, the employee receives a certain amount of points, which they can freely spend on services within the cafeteria system.

In the school area, a defined learning snack can be found as a subject for the lecture, with the help of a freely chosen or random number, in order to first receive a learning offer or a teaching assignment as a multiplier in front of the class.

Outlook: Further Democratization of Encryption through Dialogue & Open Source

As already hinted at the beginning: The transformation of the cryptography does not take place only with the described technical contents, but also with the extension of the recipient of the contents. And third, with a source-open design of the transfer.

The knowledge of the methods of encryption has reached in concentric circles more layers and knowledge carriers: It is a development from the experts of state and military institutions as knowledge carriers of cryptographic processes to scholars and students at universities and colleges as knowledge carriers to nowadays to the individuals who create encryption in companies for

customers, users and the market, or learn about it in school lessons.

The "Democratization of Cryptography"(↗) (Edwards 2019) has therefore given knowledge and experience in the Internet age to even more groups: Consultancies and actors in the many institutions of the world dealing with sensitive and protected data: They can be found e.g. in the financial world, healthcare, public and academic institutions, human rights groups, non-governmental organizations, the entertainment industry, and any open source community.

No longer political and military protectors and observers of secrets and their procedures, but mathematicians and computer scientists had and have the human right to privacy through a calculation of the truth as strong as never before in the hand.

Added to this are users of open source encryption programs that describe these in a generally understandable way for others.

In the meantime, every citizen can cryptographically secure communication and content to be transferred by programming their own software with appropriate code libraries, frameworks and compilers. With open source libraries and applications, encryption has taken a promising and necessary route among users of the Internet.

Thus, many contents and processes of the concepts described in the already mentioned open-source programming called Spot-On are provided: A very elaborate application that will produce many more research and can serve as a practical demonstration example in the classroom.

In the future, the three topics "Going-The-Extra-Mile" (↗) and the use of "Virtual Keyboard" (↗) as well as works in the sense of "Open Source" (↗) - with regard to cryptographic software, but also texts, as they can be found in Wikipedia - develop further.

- Since the encryption should not be broken or provided with back-doors, it remains only to tap the text inputs before the encryption process.

This is done on devices that have another "layer" - not to say Trojan horse (↗) - with which the written texts can be intercepted. Therefore, it is important to design the input and then encryption of text on devices that have never been on the Internet, so there is no chance that they will have a tap interface via online injection, or even text on the keyboard of the operating system could be sent unnoticed in an existing online connection to third parties.

The term "Going the Extra Mile" points to this "last mile" to a terminal that is not connected to the Internet, but can still pass the encrypted packet to a device (for example, via Bluetooth(↗)), which then performs the shipping in the regular online network. Furthermore, a virgin device of the "extra mile" also offers the option that the file containing the private key cannot easily be uploaded by attackers and encrypted text can then be converted together with the private and public key, thanks to an obtained copy of the private key from a defined storage path of the device connected to the Internet.

- "Virtual Keyboards", that are keyboards that are in the same process as the actual application (e.g. the text messenger) also provide greater security than keyboards of the operating systems that could be infected or branch off text.
- In the future, open source cryptographic software will not only be integrated into the teaching process, but its use will also be described online and thus available for every citizen.

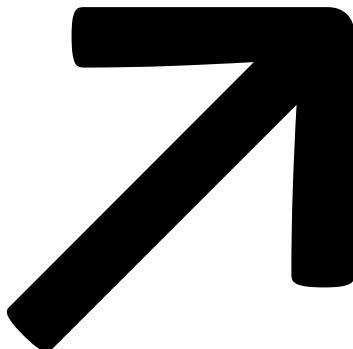
Numerous experts and editors in Wikipedia have also contributed to democratization of the knowledge of encryption processes and the security of the Internet and made available materials and texts for such presentations. They have been integrated into this book concept with their public open license. Thanks to all other et-altera-editors for the individual entries.

The book calculation is also set to zero profit, so that this knowledge work is available for everyone at a cost price comparable to an effort for a lunch meal. In addition, the authors donate any mathematically generated revenue to Wikipedia, Wikimedia, and libraries 1:1.

We wish all readers an attentive reading of all articles in the encyclopedia and recommend basically to use a pen and to mark on the sides those texts that are new or interesting for oneself or remain from the professional point of view to be debatable with others.

May these ideas allow each reader to contribute their own public article to the further development of these topics, or at least to enter into dialogue with their neighbor through the Nomenclatura - with or without the selection method of a Cryptographic Cafeteria.

Linda A. Bertram and Gunter van Dooble, July 2019.



Access Control

Access Control means to ensure that access to assets is authorized and restricted based on business and security requirements. Related to authorization of users, and assessment of rights.

AE - Adaptive Echo

The Adaptive Echo (AE) does not send - in terms of the normal Echo Protocol - a message-packet to each connected node, instead, for the over giving of a message a cryptographic token is needed. The Echo-Protocol is equipped for the Adaptive Echo modus with a routing information. Only nodes which have a certain cryptographic token available get the message forwarded.

In order to explain the Adaptive Echo, the fairy tale of "Hansel and Gretel" can serve as a classic example. The people Hansel, Gretel and the evil witch are shown as nodes in the below-mentioned AE grid. Now, Hansel and Gretel consider how they can communicate with each other without the evil witch recognizing this. According to the fairy tale they are in the forest with the witch and want to find out again from this forest and mark the way with "breadcrumbs" and "white pebbles". If nodes A2, E5, and E2 use the same AE token within an Echo Network, node E6 will not receive any message that node A2 (Hansel) and node E2 (Gretel) will exchange. The Cryptographic Token (Password) "breadcrumbs" steers the routing of the message packet. The Adaptive Echo Protocol has been implemented in the application Spot-on Encryption Suite and GoldBug Crypto Messenger.

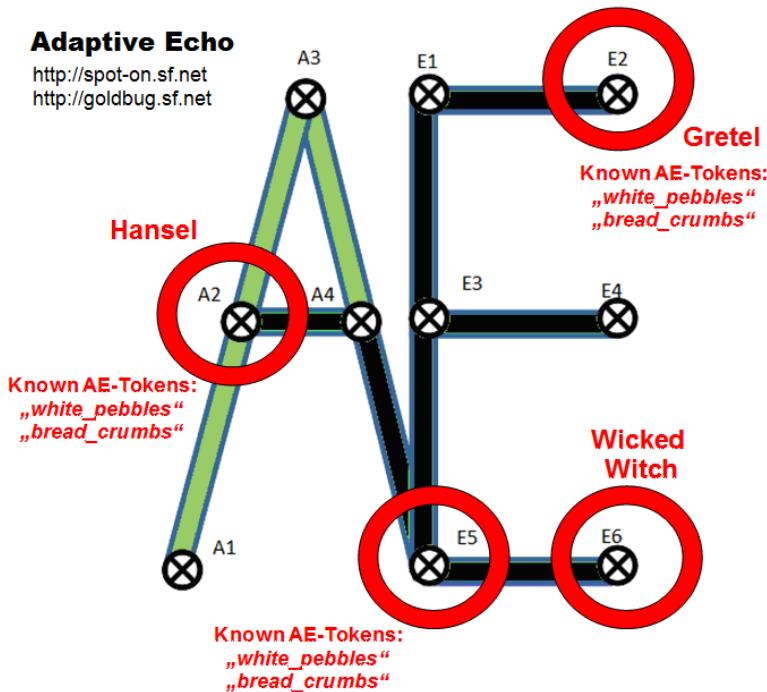


Figure 1: Adaptive Echo Template [PD]

AES - Advanced Encryption Standard

The Advanced Encryption Standard (AES), also known as Rijndael (its former original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption

Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES is based on a design principle known as a substitution–permutation network and is efficient in both software and hardware. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael per se is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits. AES operates on a 4×4 column-major order array of bytes, termed the state. Most AES calculations are done in a particular finite field. Unlike its predecessor DES, AES does not use a Feistel network. A Feistel cipher is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel who did pioneering research while working for IBM (USA); it is also commonly known as a Feistel network. A large proportion of block ciphers use the scheme, including the Data Encryption Standard (DES). The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore, the size of the code or circuitry required to implement such a cipher is nearly halved. Hence, a Feistel network is an iterated cipher with an internal function called a round function.

The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext.

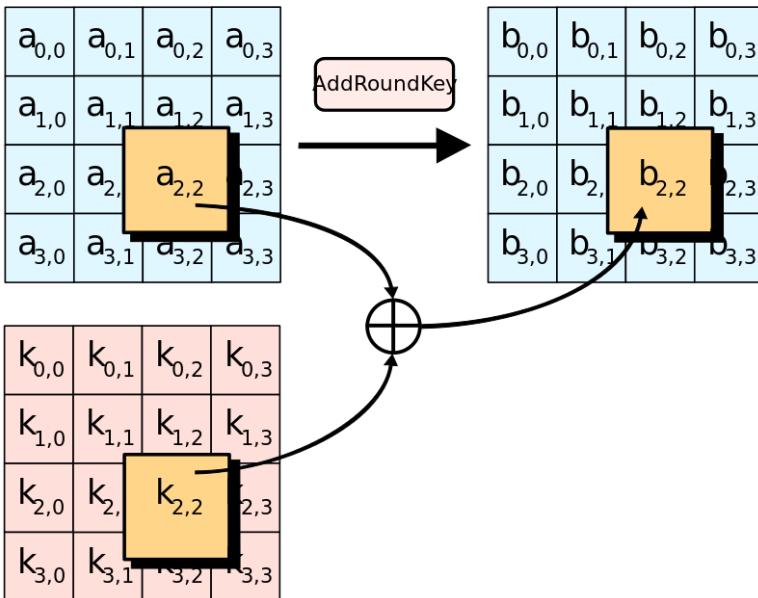


Figure 2: AddRoundKey step within the AES creation [PD]

In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XOR operation (\oplus).

The number of rounds is as follows: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, 14 rounds for 256-bit keys. Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. SubBytes defines a non-linear substitution step where each byte is replaced with another according to a lookup table. ShiftRows defines a transposition step where the last three rows of the state are shifted cyclically a certain number of steps. MixColumns defines a linear mixing operation which

operates on the columns of the state, combining the four bytes in each column. For AddRoundKey the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

AE-Token

The AE-Token is a cryptographic token used to deploy the Adaptive Echo (AE) modus. It is a kind of password or string, which is entered into the node, to avoid messages to be sent to nodes, without the AE-Token. AE-Tokens can help to create a self-learning, adaptive network. The token must contain at least thirty-six characters.

Algorithm

In mathematics and computer science, an algorithm is a self-contained step-by-step set of operations to be performed. Algorithms exist that perform calculation, data processing, and automated reasoning.

Flowchart of an algorithm (Euclid's algorithm) for calculating the greatest common divisor (g.c.d.) of two numbers a and b in locations named A and B. In mathematics, the Euclidean algorithm, or Euclid's algorithm, is an efficient method for computing the greatest common divisor (GCD) of two numbers, the largest number that divides both of them without leaving a remainder. It is named after the ancient Greek mathematician Euclid, who first described it in his Elements (c. 300 BC). It is an example of an algorithm, a step-by-step procedure for performing a calculation according to well-defined rules and is one of

the oldest algorithms in common use. The algorithm proceeds by successive subtractions in two loops: IF the test $B \geq A$ yields "yes" (or true) (more accurately the number b in location B is greater than or equal to the number a in location A) THEN, the algorithm specifies $B \leftarrow B - A$ (meaning the number $b - a$ replaces the old b). Similarly, IF $A > B$, THEN $A \leftarrow A - B$. The process terminates when (the contents of) B is 0, yielding the g.c.d. in A .

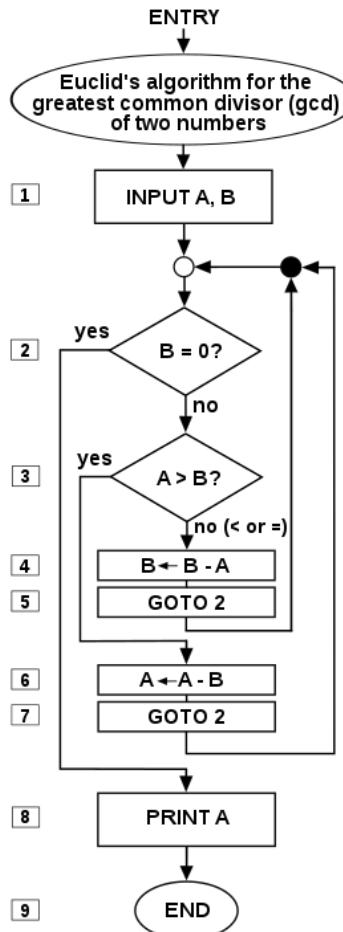


Figure 3: Flowchart of Euclid's algorithm [SA4]

Alice and Bob

Alice and Bob are the names of fictional characters used for convenience and to aid comprehension. For example, "How can Bob send a private message M to Alice in a public-key cryptosystem?" is believed to be easier to describe and understand than "How can B send a private message M to A in a public-key cryptosystem?" In cryptography and computer security, Alice and Bob are used extensively as participants in discussions about cryptographic protocols or systems. The names are conventional, and other than Alice and Bob often use a rhyming mnemonic to associate the name with the typical role of that person. The first mention of Alice and Bob in the context of cryptography was in Rivest, Shamir, and Adleman's 1978 article "A method for obtaining digital signatures and public-key cryptosystems". They wrote: "For our scenarios we suppose that A and B (also known as Alice and Bob) are two users of a public-key cryptosystem" (p. 121). Previous to this article, cryptographers typically referred to message senders and receivers as A and B, or other simple symbols.

Android

Android is a mobile operating system developed by Google. It is based on a modified version of the Linux kernel and other open source software and is designed primarily for touchscreen mobile devices such as smartphones and tablets. Android has been the best-selling OS worldwide on smartphones since 2011 and on tablets since 2013.

The mobile operating system allows to deploy mobile devices similar as an Raspberry Pi with server software, e.g. like the encrypting chat server SmokeStack for Android. Based on the Android mobile platform LineageOS is a free and open-source operating system for set-top boxes, smartphones and tablet computers, free of connections to and services from Google.

Anonymity

Anonymity, adjective "anonymous", is derived from the Greek word ἀνώνυμία, anonymia, meaning "without a name" or "namelessness". In colloquial use, "anonymous" is used to describe situations where the acting person's name is unknown. Some writers have argued that namelessness, though technically correct, does not capture what is more centrally at stake in contexts of anonymity. The important idea here is that a person be non-identifiable, unreachable, or untrackable. Anonymity is seen as a technique, or a way of realizing, certain other values, such as privacy, or liberty. An important example for anonymity being not only protected but enforced by law is the vote in free elections. In many other situations (like conversation between strangers, buying some product or service in a shop), anonymity is traditionally accepted as natural. There are also various situations in which a person might choose to withhold their identity. Acts of charity have been performed anonymously when benefactors do not wish to be acknowledged. A person who feels threatened might attempt to mitigate that threat through anonymity. A witness to a crime might seek to avoid

retribution, for example, by anonymously calling a crime tipline. Criminals might proceed anonymously to conceal their participation in a crime. Anonymity may also be created unintentionally, through the loss of identifying information due to the passage of time or a destructive event. The term "anonymous message" typically refers to a message that does not reveal its sender. In many countries, anonymous letters are protected by law and must be delivered as regular letters. In mathematics, in reference to an arbitrary element (e.g., a human, an object, a computer), within a well-defined set (called the "anonymity set"), "anonymity" of that element refers to the property of that element of not being identifiable within this set. If it is not identifiable, then the element is said to be "anonymous."

Answer Method

The Answer Method is a procedure for the login into an application. It is applied in the software Spot-On and GoldBug. Here the login into the application can be done over a password, or, the password is replaced by two entry text fields. One string covers the question, and the other string covers the referring answer to the question. Both values are hashed and processed in a cryptographic way. The right answers are not stored (as a hash of it) on the hard disk in plaintext, so that the process provides a different method than the normal login procedure and offers more security. An attacker does not know, if a user has used the password or the question/answer login

method, as both methods are given as choice for the above-mentioned applications.

Asymmetric Calling

Cryptographic Calling is the immediate transfer of end-to-end encrypting encryption credentials to secure a communication channel. Cryptographic Calling has been invented by the Software Project Spot-On. Asymmetric Calling is some modus for Cryptographic Calling, which sends temporary asymmetric keys for end-to-end encryption. It refers to send one asymmetric key (pair) through one secured channel. The Call with asymmetric credentials refers to ephemeral asymmetric keys, which are used for the time of the call. This could be one session or even a shorter part of time of the session. It depends whenever a communication partner starts to initiate a call. The asymmetric ephemeral credentials for the call should be transferred over a secure connection, which is either defined by a symmetric key, sends over an a-symmetric key (PKI) or over an already existent call-connection, in this (above mentioned) case an ephemeral asymmetric temp-key.

Asymmetric Encryption

Asymmetric encryption, or public-key cryptography, is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. The generation of such keys

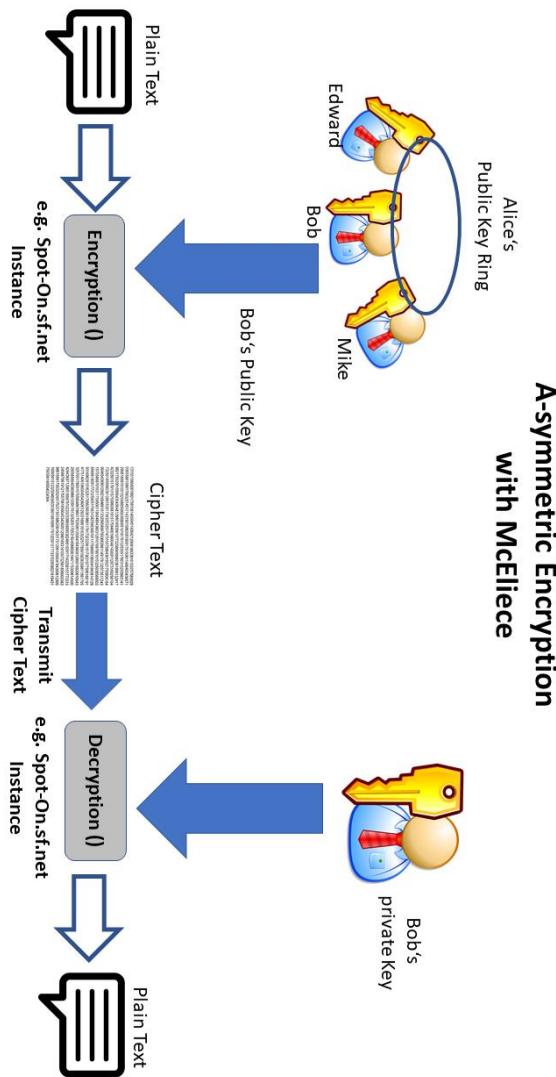


Figure 4: How asymmetric encryption with Public Key Infrastructure (PKI) works [PD]

depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security. In such a system, any person can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key. Robust authentication is also possible. A sender can combine a message with a private key to create a short digital signature on the message. Anyone with the corresponding public key can combine a message, a putative digital signature on it, and the known public key to verify whether the signature was valid, i.e. made by the owner of the corresponding private key. Public key algorithms are fundamental security ingredients in modern cryptosystems, applications and protocols assuring the confidentiality, authenticity and non-repudiability of electronic communications and data storage. They underpin various Internet standards, such as Transport Layer Security (TLS), S/MIME, OpenPGP, and GPG. Some public key algorithms provide key distribution and secrecy (e.g., Diffie–Hellman key exchange), some provide digital signatures (e.g., Digital Signature Algorithm), and some provide both (e.g., RSA).

Attack

An attack is an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Audit

An audit is a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines). An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement. A software audit review, or software audit, is a type of software review in which one or more auditors who are not members of the software development organization conduct an independent examination of a software product, software process, or set of software processes to assess compliance with specifications, standards, contractual agreements, or other criteria. "Software product" mostly, but not exclusively, refers to some kind of technical document. (e.g. IEEE Std. 1028 offers a list of 32 examples of software products subject to audit, including documentary products such as various sorts of plan, contracts, specifications, designs, procedures, standards, and reports, but also non-documentary products such as data, test data, and deliverable media). Software audits are distinct from software peer reviews and software

management reviews in that they are conducted by personnel external to, and independent of, the software development organization, and are concerned with compliance of products or processes, rather than with their technical content, technical quality, or managerial implications. The following principles of an technology audit should find a reflection: (1) *Timeliness*: Only when the processes and programming is continuously inspected in regard to their potential susceptibility to faults and weaknesses, but as well with regard to the continuation of the analysis of the found strengths, or by comparative functional analysis with similar applications an updated frame can be continued. (2) *Source openness*: It requires an explicit reference in the audit of encrypted programs, how the handling of open source has to be understood. E.g. programs, offering an open source application, but not considering the IM server as open source, have to be regarded as critical. An auditor should take an own position to the paradigm of the need of the open source nature within cryptologic applications. (3) *Elaborateness*: Audit processes should be oriented to certain minimum standard. The recent audit processes of encrypting software often vary greatly in quality, in the scope and effectiveness and also experience in the media reception often differing perceptions. Because of the need of special knowledge on the one hand and to be able to read programming code and then on the other hand to also have knowledge of encryption procedures, many users even trust the shortest statements of formal confirmation. Individual commitment as an auditor, e.g. for quality, scale and effectiveness, is thus to be assessed reflexively for yourself and to be

documented within the audit. (4) *The financial context:* Further transparency is needed to clarify whether the software has been developed commercially and whether the audit was funded commercially (paid Audit). It makes a difference whether it is a private hobby / community project or whether a commercial company is behind it. (5) *Scientific referencing of learning perspectives:* Each audit should describe the findings in detail within the context and also highlight progress and development needs constructively. An auditor is not the parent of the program, but at least he or she is in a role of a mentor, if the auditor is regarded as part of a PDCA learning circle (PDCA = Plan-Do-Check-Act). There should be next to the description of the detected vulnerabilities also a description of the innovative opportunities and the development of the potentials. (6) *Literature-inclusion:* A reader should not rely solely on the results of one review, but also judge according to a loop of a management system (e.g. PDCA, see above), to ensure, that the development team or the reviewer was and is prepared to carry out further analysis, and also in the development and review process is open to learnings and to consider notes of others. A list of references should be accompanied in each case of an audit. (7) *Inclusion of user manuals & documentation:* Further a check should be done, whether there are manuals and technical documentations, and, if these are expanded. (8) *Identify references to innovations:* Applications with innovative features should be tested with high priority (e.g. applications that allow both, messaging to offline and online contacts, so considering chat and e-mail in one application - as it is also the case e.g. with the GoldBug Chat & E-Mail application).

And: The auditor should also highlight the references to innovations and underpin further research and development needs.

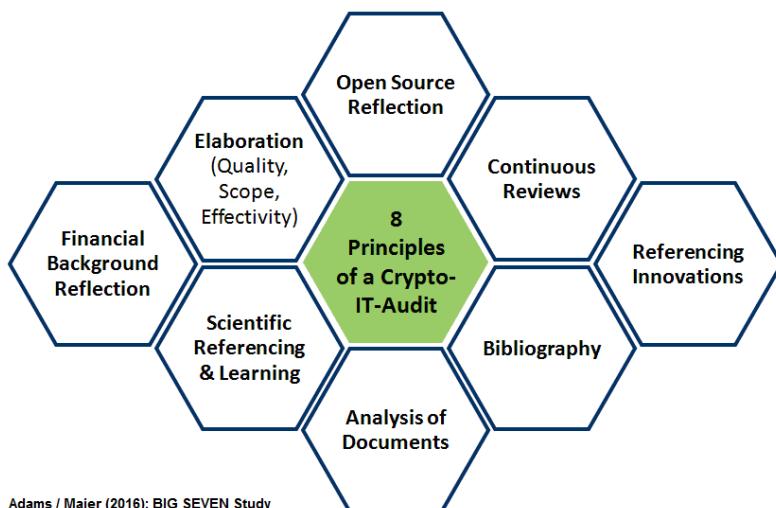


Figure 5: Eight Principles of an IT Audit of cryptographic applications [PD/SA4]

The list of audit principles for cryptographic applications by Adams/Maier (2016) describes - beyond the methods of technical analysis - particularly core values, that should be considered within a software audit.

Authentication

Authentication (from Greek: αὐθεντικός authentikos, "real, genuine", from αὐθέντης authentes, "author") is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. In contrast with identification, which refers to the act of stating or otherwise indicating a

claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the authenticity of a website with a digital certificate, determining the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification. The term digital authentication, also known as electronic authentication, refers to a group of processes where the confidence for user identities is established and presented via electronic methods to an information system. It is also referred to as e-authentication. The digital authentication process creates technical challenges because of the need to authenticate individuals or entities remotely over a network. The American National Institute of Standards and Technology (NIST) has created a generic model for digital authentication that describes the processes that are used to accomplish secure authentication: (1) *Enrollment* – an individual applies to a credential service provider (CSP) to initiate the enrollment process. After successfully proving the applicant's identity, the CSP allows the applicant to become a subscriber. (2) *Authentication* – After becoming a subscriber, the user receives an authenticator e.g., a token and credentials, such as a username. He or she is then permitted to perform online transactions within an authenticated session with a relying party, where they must provide proof that he or she possesses one or more authenticators. (3) *Life-cycle maintenance* – the CSP is charged with the task of maintaining the user's credential

of the course of its lifetime, while the subscriber is responsible for maintaining his or her authenticator(s).

The authentication of information can pose special problems with electronic communication, such as vulnerability to man-in-the-middle attacks, whereby a third party taps into the communication stream, and poses as each of the two other communicating parties, in order to intercept information from each. Extra identity factors can be required to authenticate each party's identity.

Authorization

Authorization is the function of specifying access rights/privileges to resources, which is related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define an access policy. For example, human resources staff are normally authorized to access employee records and this policy is usually formalized as access control rules in a computer system. During operation, the system uses the access control rules to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected). Resources include individual files or an item's data, computer programs, computer devices and functionality provided by computer applications. Examples of consumers are computer users, computer Software and other Hardware on the computer.

AutoCrypt

AutoCrypt is an automatic key exchange. This has originally been invented by the Spot-on Project and refers to the protocol definitions of a REPLEO and the EPKS protocol. A REPLEO is the method to encrypt the own public key with the received public key of a friend. That hides the own public key from public by using an encryption method. The EPKS Protocol is the Echo Public Key Sharing Protocol, which allows to send the own key over an existing encrypted connection to one or several friends. The EPKS protocol has been invented in the Spot-On project and GoldBug Project and has been overtaken by other projects in an automated way for an e-mail reply with public keys. That means two users of the same e-mail client exchange the public encryption key and are from that point of time secured for all further communication. The EPKS Protocol provided this many years before the Term AutoCrypt went public. Other project also copied this invention under the Name KeySync. The new process is, that the key is not stored and searched on a Key server, but sent from node to node in a secure channel, either by manual sent-out or an automated exchange of two nodes, e.g. e-mail-clients or Spot-On Clients over the EPKS protocol. EPKS automatically integrates within an EPKS-Community the shared public keys.

Availability

In reliability theory and reliability engineering, the term availability has the following meanings: The degree to

which a system, subsystem or equipment is in a specified operable and committable state at the start of a mission, when the mission is called for at an unknown, i.e. a random, time. Simply put, availability is the proportion of time a system is in a functioning condition. This is often described as a mission capable rate. Mathematically, this is expressed as 100% minus unavailability. The ratio of (a) the total time a functional unit is capable of being used during a given interval to (b) the length of the interval. For example, a unit that is capable of being used 100 hours per week (168 hours) would have an availability of 100/168. However, typical availability values are specified in decimal (such as 0.9998). In high availability applications, a metric known as nines, corresponding to the number of nines following the decimal point, is used. With this convention, "five nines" equals 0.99999 (or 99.999%) availability.

Backdoor

A backdoor is a method, often secret, of bypassing normal authentication or encryption in a computer system, a product, or an embedded device (e.g. a home router), or its embodiment, e.g. as part of a cryptosystem, an algorithm, a chipset, or a "homunculus computer" — a tiny computer-within-a-computer (such as that found in Intel's AMT technology). Backdoors are often used for securing remote access to a computer, or obtaining access to plaintext in cryptographic systems. The backdoor may be used to gain access to passwords, delete data on hard drives, or transfer information within the cloud. A backdoor may take the form of a hidden part of a program, a separate program

(e.g. Back Orifice may subvert the system through a rootkit), code in the firmware of the hardware, or parts of an operating system such as Windows. Trojan horses can be used to create vulnerabilities in a device. In 1993, the United States government attempted to deploy an encryption system, the Clipper chip, with an explicit backdoor for law enforcement and national security access. The chip was unsuccessful. In January 2014, a backdoor was discovered in certain Samsung Android products, like the Galaxy devices. The Samsung proprietary Android versions are fitted with a backdoor that provides remote access to the data stored on the device. In particular, the Samsung Android software that is in charge of handling the communications with the modem, using the Samsung IPC protocol, implements a class of requests known as remote file server (RFS) commands, that allows the backdoor operator to perform via modem remote I/O operations on the device hard disk or other storage. As the modem is running Samsung proprietary Android software, it is likely that it offers over-the-air remote control that could then be used to issue the RFS commands and thus to access the file system on the device.

10 Trends in Crypto Messaging

A Study on the open source Applications GoldBug, CryptoCat, OTR+XMPP, RetroShare, Signal, Surespot and Tox.



Adams, D. / Maier, A.K. (2016)

Figure 6: 10 Trends in Cryptographic Messaging (2016) [PD]

Big Seven Study (2016)

Big Seven Study (2016) is a report on open source encrypting Messengers integrated into an IT and code audit of the Messenger GoldBug (v2.7). The two security researchers David Adams (Tokyo) and Ann-Kathrin Maier (Munich), who examined in their BIG SEVEN study seven well-known encryption applications for e-mail and instant messaging out of the open source area, performed then a deeper IT-audit for the acquainted software solution GoldBug.sf.net. The audit took into account the essential criteria, study fields and methods on the basis of eight international IT-audit manuals and was carried out in 20 dimensions. The software "GoldBug – e-mail client and instant messenger" here was ahead with excellent results and is not only very trustworthy and compliant to international IT-audit manuals and safety standards, GoldBug also scores in comparison and in the evaluation of the single functions in much greater detail than the other comparable open source crypto messenger. Numerous details have been analysed by various methods, compared and also strategically evaluated by the two authors regarding the current encryption discussions. The comparatively studied applications include CryptoCat, GoldBug, OTR-XMPP clients such as Pidgin with the OTR-plugin, RetroShare and Signal, Surespot and Tox. This selection was based on a full list of all encrypting software that could be found by several researchers and portals at that time. A synopsis of all these encrypting messengers has been made within this study and the chosen seven application remained as to be searched deeper. After the institute NIST (Chen et al.) has stated in February 2016 that

the algorithm RSA in quantum computer age is broken respectively no longer sure, GoldBug is the remaining Messenger which has next to RSA also even ElGamal, McEliece and NTRU Algorithms implemented and therefore can be regarded as safe against Quantum computers! The in-depth audit was therefore carried out for this of seven Messengers. Therefore, the comparative BIG SEVEN study about open source crypto-messaging respective the GoldBug audit-report is recommended not only as a resource for IT interested readers, students, mathematicians, cryptologists and auditors, but also can be regarded as a basis for discussion on further development in the field of research, programming and as preparatory reading material for questions at the next crypto party. The study has been archived accordingly at the project and can be downloaded at the following URL:
<https://sf.net/projects/goldbug/files/bigseven-crypto-audit.pdf>

Biometric Passport

A biometric passport (also known as an e-passport, ePassport, or a digital passport) is a traditional passport that has an embedded electronic microprocessor chip which contains biometric information that can be used to authenticate the identity of the passport holder. It uses contactless smart card technology, including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or center page, of the passport. The passport's critical information is both printed on the data

page of the passport and stored in the chip. Public key infrastructure (PKI) is used to authenticate the data stored electronically in the passport chip making it expensive and difficult to forge when all security mechanisms are fully and correctly implemented. Many countries are moving towards the issue of biometric passports. Privacy proponents in many countries question and protest the lack of information about exactly what the passports' chip will contain, and whether they impact civil liberties. The main problem they point out is that data on the passports can be transferred with wireless RFID technology, which can become a major vulnerability. Although this could allow ID-check computers to obtain a person's information without a physical connection, it may also allow anyone with the necessary equipment to perform the same task. If the personal information and passport numbers on the chip are not encrypted, the information might wind up in the wrong hands.

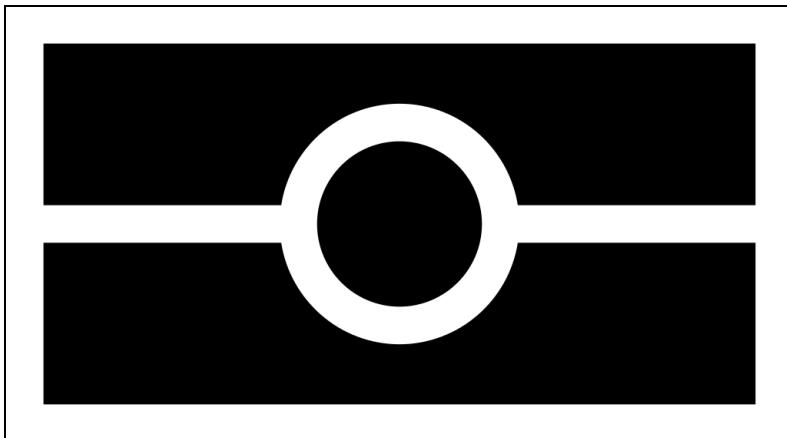


Figure 7: Symbol on the cover of biometric passports [PD]

Birthday Problem

In probability theory, the birthday problem or birthday paradox concerns the probability that, in a set of n randomly chosen people, some pair of them will have the same birthday. By the pigeonhole principle, the probability reaches 100% when the number of people reaches 367 (since there are only 366 possible birthdays, including February 29). However, 99.9% probability is reached with just 70 people, and 50% probability with 23 people. These conclusions are based on the assumption that each day of the year (excluding February 29) is equally probable for a birthday. It may well seem surprising that a group of just 23 individuals is required to reach a probability of 50% that two individuals in the group have the same birthday: this result is perhaps made more plausible by considering that the comparisons of birthday will actually be made between every possible pair of individuals = $23 \times 22/2 = 253$ comparisons, which is well over half the number of days in a year (183 at most), as opposed to fixing on one individual and comparing their birthday to everyone else's birthday. Real-world applications for the birthday paradox include a cryptographic attack called the birthday attack, which uses this probabilistic model to reduce the complexity of finding a collision for a hash function.

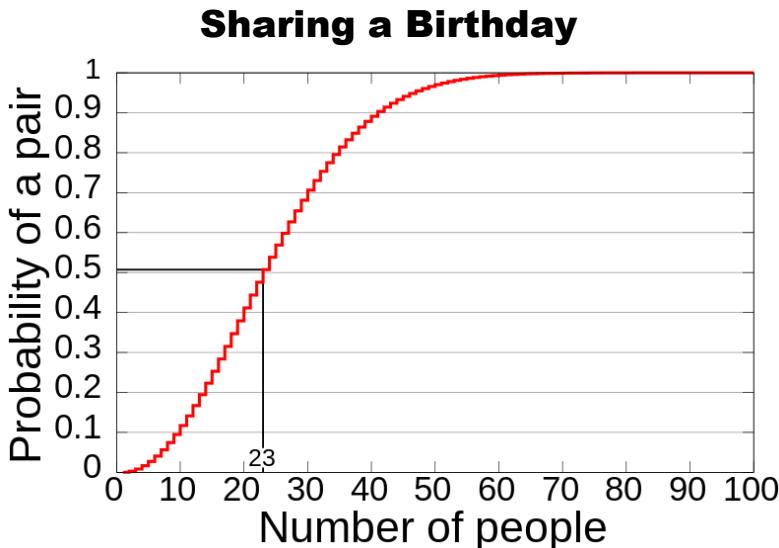


Figure 8: Probability of at least two people sharing a birthday [SA3]

The computed probability of at least two people sharing a birthday versus the number of people.

Blinding

Blinding is a technique in cryptography by which an agent can provide a service to (i.e., compute a function for) a client in an encoded form without knowing either the real input or the real output. Blinding techniques also have applications to preventing side-channel attacks on encryption devices. More precisely, Alice has an input x and Oscar has a function f . Alice would like Oscar to compute $y = f(x)$ for her without revealing either x or y to him. The reason for her wanting this might be that she doesn't know the function f or that she does not have the resources to

compute it. Alice "blinds" the message by encoding it into some other input $E(x)$; the encoding E must be a bijection on the input space of f , ideally a random permutation. In mathematics, a bijection or one-to-one correspondence, is a function between the elements of two sets, where each element of one set is paired with exactly one element of the other set, and each element of the other set is paired with exactly one element of the first set. There are no unpaired elements. Oscar gives her $f(E(x))$, to which she applies a decoding D to obtain $D(f(E(x))) = y$. The most common application of blinding is the blind signature. A blind signature is a form of digital signature in which the content of a message is disguised (blinded) before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message in the manner of a regular digital signature. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes. In a blind signature protocol, the signer digitally signs a message without being able to learn its content. The one-time pad (OTP) is an application of blinding to the secure communication problem, by its very nature. Alice would like to send a message to Bob secretly, however all of their communication can be read by Oscar. Therefore, Alice sends the message after blinding it with a secret key or OTP that she shares with Bob. Bob reverses the blinding after receiving the message. In this example, the function f is the identity and E and D are both typically the XOR operation.

Block Cipher

A block cipher is a deterministic algorithm operating on fixed-length groups of bits, called a block, with an unvarying transformation that is specified by a symmetric key. Block ciphers operate as important elementary components in the design of many cryptographic protocols and are widely used to implement encryption of bulk data.

The modern design of block ciphers is based on the concept of an iterated product cipher. In his seminal 1949 publication, *Communication Theory of Secrecy Systems*, Claude Shannon analysed product ciphers and suggested them as a means of effectively improving security by combining simple operations such as substitutions and permutations. Many other realizations of block ciphers, such as the AES, are classified as substitution-permutation networks. Even a secure block cipher is suitable only for the encryption of a single block under a fixed key. A multitude of modes of operation have been designed to allow their repeated use in a secure way, commonly to achieve the security goals of confidentiality and authenticity. However, block ciphers may also feature as building blocks in other cryptographic protocols, such as universal hash functions and pseudo-random number generators. A block cipher consists of two paired algorithms, one for encryption, E , and the other for decryption, D . Both algorithms accept two inputs: an input block of size n bits and a key of size k bits; and both yield an n -bit output block. The decryption algorithm D is defined to be the inverse function of encryption, i.e., $D = E^{-1}$.

A block cipher by itself allows encryption only of a single data block of the cipher's block length. For a variable-length

message, the data must first be partitioned into separate cipher blocks. In the simplest case, known as the Electronic Codebook (ECB) mode, a message is first split into separate blocks of the cipher's block size (possibly extending the last block with padding bits), and then each block is encrypted and decrypted independently. However, such a naive method is generally insecure because equal plaintext blocks will always generate equal ciphertext blocks (for the same key), so patterns in the plaintext message become evident in the ciphertext output.

To overcome this limitation, several so-called block cipher modes of operation have been designed and specified in national recommendations such as NIST 800-38A and BSI TR-02102 and international standards such as ISO/IEC 10116. The general concept is to use randomization of the plaintext data based on an additional input value, frequently called an initialization vector, to create what is termed probabilistic encryption. In the popular cipher block chaining (CBC) mode, for encryption to be secure the initialization vector passed along with the plaintext message must be a random or pseudo-random value, which is added in an exclusive-or manner to the first plaintext block before it is being encrypted. The resultant ciphertext block is then used as the new initialization vector for the next plaintext block.

Some modes such as the CBC mode only operate on complete plaintext blocks. Simply extending the last block of a message with zero-bits is insufficient since it does not allow a receiver to easily distinguish messages that differ only in the amount of padding bits.

In the cipher feedback (CFB) mode, which emulates a self-synchronizing stream cipher, the initialization vector is first encrypted and then added to the plaintext block. The output feedback (OFB) mode repeatedly encrypts the initialization vector to create a key stream for the emulation of a synchronous stream cipher. The newer counter (CTR) mode similarly creates a key stream, but has the advantage of only needing unique and not (pseudo-)random values as initialization vectors; the needed randomness is derived internally by using the initialization vector as a block counter and encrypting this counter for each block.

Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices and building personal area networks (PANs).

Botan

Botan is a BSD-licensed cryptographic library written in C++. It provides a wide variety of cryptographic algorithms, formats, and protocols, e.g. SSL and TLS. It is used in the Monotone distributed revision control program, the OpenDNSSEC system, and ISC's Kea DHCP server among other projects. The project was originally called OpenCL, a name now used by Apple Inc. and Khronos Group for a heterogeneous system programming framework. It was

renamed Botan in 2002. In 2007, the German Federal Office for Information Security contracted FlexSecure GmbH to add an implementation of Card Verifiable Certificates for ePassports to Botan; the modified version of Botan was released under the name InSiTo. Starting in 2015, the German Federal Office for Information Security funded a project which included improving the documentation, test suite and feature set of Botan, culminating in 2017 when it was evaluated and recommended as a library suitable for applications with increased security requirements.

Bouncy Castle

Bouncy Castle is a collection of APIs used in cryptography. It includes APIs for both the Java and the C# programming languages. The APIs are supported by a registered Australian charitable organization: Legion of the Bouncy Castle Inc. Bouncy Castle is Australian in origin and therefore American regulations from the United States do not apply to it. Bouncy Castle started when two colleagues were tired of having to re-invent a set of cryptography libraries each time they changed jobs working in server-side Java SE. One of the developers was active in Java ME (J2ME at that time) development as a hobby and a design consideration was to include the greatest range of Java VMs for the library, including those on J2ME. This design consideration led to the architecture that exists in Bouncy Castle. The project was founded in May 2000. It was originally just Java. C# API added in 2004. The original Java API consisted of approximately 27,000 lines of code,

including test code and provided support for J2ME, a JCE/JCA provider, and basic X.509 certificate generation.

Broadcast (in Cryptography)

Broadcast is a term widely known. In Cryptography it is known from the Spot-On application to send the public encryption key over an IP-network connection, so that all connected nodes can pick-up the sent key. A cryptographic Broadcast is a wider form of AutoCrypt and includes as well the EPKS channel. It is also possible to send the Cryptographic Broadcast over a not encrypted connection, while a broadcast over the Echo Network or the Echo Public Key Sharing function of the Spot-On Client would provide always an encrypted connection, e.g. based on the symmetric key: only people who know the key have then in this case access to the broadcast of e.g. further keys, messages or files.

Brute-force Attack

A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search. A brute-force attack is a cryptanalytic attack that can, in theory, be used to attempt to decrypt any encrypted data (except for data encrypted in

an information-theoretically secure manner). Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. When password-guessing, this method is very fast when used to check all short passwords, but for longer passwords other methods such as the dictionary attack are used because a brute-force search takes too long. Longer passwords, passphrases and keys have more possible values, making them exponentially more difficult to crack than shorter ones. Brute-force attacks can be made less effective by obfuscating the data to be encoded making it more difficult for an attacker to recognize when the code has been cracked or by making the attacker do more work to test each guess. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to mount a successful brute-force attack against it. Brute-force attacks are an application of brute-force search, the general problem-solving technique of enumerating all candidates and checking each one.

Bullrun (Decryption Program)

Bullrun (stylized BULLRUN) is a clandestine, highly classified program to crack encryption of online communications and data, which is run by the United States National Security Agency (NSA). The British Government Communications Headquarters (GCHQ) has a similar program codenamed Edgehill. According to the BULLRUN classification guide published by The Guardian, the program uses multiple methods including computer network exploitation,

interdiction, industry relationships, collaboration with other intelligence community entities, and advanced mathematical techniques. Information about the program's existence was leaked in 2013 by Edward Snowden. Snowden claims according to Neal and Kerner (2013) that since 2011, expenses devoted to Bullrun amount to \$800 million. The leaked documents reveal that Bullrun seeks to defeat the encryption used in specific network communication technologies.

Button

A button is the most discussed element in an application, respective the GUI development.

Buzz / e*IRC

Buzz is the name of the libspoton function to provide Echoed/Encrypted IRC (e*IRC). So, Buzz is another word for IRC, respective e*IRC, used by this library respective kernel. Buzz is a model for encrypted IRC chat within groups. Each user knowing a Magnet-URI link with cryptographic values is able to read the encrypted group chat. The privacy of two users in the group for 1:1 chat depends on how secret this Magnet-URI link has been kept, as it is based on symmetric encryption (e.g. AES encryption).

C/O - (Care-of)-Function

“Care of”, used to address a letter when the letter must pass through an intermediary (also written C/O). Neighbors are often asked to care of your postal letters, in case you live with them in one house or have a relationship to them. As well parcel stations, letter boxes or just persons e.g. at your home or in the neighborhood provide a local delay of your envelopes and parcels, in case you are at work and want to receive the parcel or letter in the evening. The included e-mail function of Spot-On provides such a feature.

CBC - Cipher Block Chaining

Cipher Block Chaining – Ehrsam, Meyer, Smith and Tuchman invented the Cipher Block Chaining (CBC) mode of operation in 1976. In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. Many modes of operation have been defined, CBC is only a popular one. Some of these further block cipher modes of operation are described in the table below. The purpose of cipher modes is to mask patterns which exist in encrypted data.

Mode	Formulas	Ciphertext
Electronic Codebook (ECB)	$Y_i = F(PlainText_i, Key)$	Y_i
Cipher Block Chaining (CBC)	$Y_i = PlainText_i \text{ XOR } Ciphertext_{i-1}$	$F(Y.key), Ciphertext_0 = IV$
Propagating CBC (PCBC)	$Y_i = PlainText_i \text{ XOR } (Ciphertext_{i-1} \text{ XOR } PlainText_{i-1})$	$F(Y.key), Ciphertext_0 = IV$
Cipher Feedback (CFB)	$Y_i = Ciphertext_{i-1}$	Plaintext XOR $F(Y.key); Ciphertext_0 = IV$
Output Feedback (OFB)	$Y_i = F(Key, Y_{i-1}), Y_0 = IV$	Plaintext XOR Y_i
Counter (CTR)	$Y_i = F(Key, IV + g(i)); IV = token();$	Plaintext XOR Y_i

Caesar Cipher

A Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques.

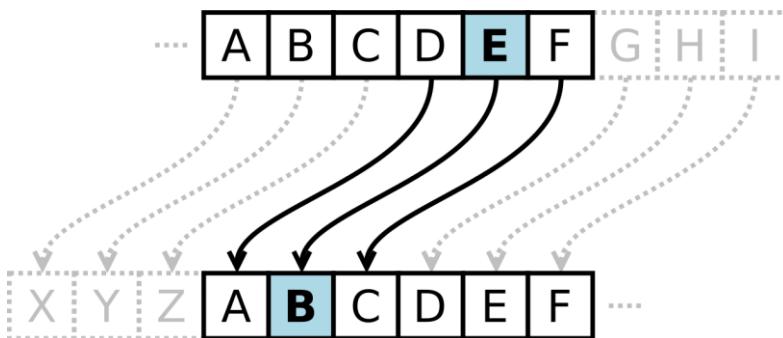


Figure 9: The Caesar cipher [PD]

The action of a Caesar cipher is to replace each plaintext letter with a different one a fixed number of places down the alphabet. The cipher illustrated here uses a left shift of three, so that (for example) each occurrence of E in the plaintext becomes B in the ciphertext.

It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence. The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes, such as the Vigenère cipher, and still has modern application in the ROT13 system. As with all single-alphabet substitution ciphers, the Caesar cipher is easily

broken and in modern practice offers essentially no communications security.

The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by some number of positions. For instance, here is a Caesar cipher using a left rotation of three places, equivalent to a right shift of 23 (the shift parameter is used as the key):

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: XYZABCDEFGHIJKLMNPQRSTUVWXYZ

When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line.

Plaintext:

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Ciphertext:

QEB NRFZH YOLTQ CLU GRJMP LSBO QEB IXWV ALD

Deciphering is done in reverse, with a right shift of 3.



Figure 10: Two rotating disks with a Caesar cipher [PD]

A construction of two rotating disks with a Caesar cipher can be used to encrypt or decrypt the code.

Certificate Authority

A certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the

private key that corresponds to the certified public key. A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 standard. One particularly common use for certificate authorities is to sign certificates used in HTTPS, the secure browsing protocol for the World Wide Web. Another common use is in issuing identity cards by national governments for use in electronically signing documents. If the CA can be subverted, then the security of the entire system is lost, potentially subverting all the entities that trust the compromised CA.

Chaos Theory

Chaos theory is a branch of mathematics focusing on the behavior of dynamical systems that are highly sensitive to initial conditions. "Chaos" is an interdisciplinary theory stating that within the apparent randomness of chaotic complex systems, there are underlying patterns, constant feedback loops, repetition, self-similarity, fractals, self-organization, and reliance on programming at the initial point known as sensitive dependence on initial conditions. The butterfly effect describes how a small change in one state of a deterministic nonlinear system can result in large differences in a later state, e.g. a butterfly flapping its wings in Brazil can cause a hurricane in Texas. Small differences in initial conditions, such as those due to rounding errors in numerical computation, yield widely diverging outcomes for such dynamical systems, rendering long-term prediction of their behavior impossible in general. This happens even

though these systems are deterministic, meaning that their future behavior is fully determined by their initial conditions, with no random elements involved. In other words, the deterministic nature of these systems does not make them predictable. This behavior is known as deterministic chaos, or simply chaos.

Cipher

In cryptography, a cipher is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure. An alternative, less common term is encipherment. To encipher or encode is to convert information into cipher or code. In common parlance, ‘cipher’ is synonymous with ‘code’. Codes generally substitute different length strings of characters in the output, while ciphers generally substitute the same number of characters as are input.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 11: Tabula recta [PD]

All polyalphabetic ciphers based on Caesar ciphers can be described in terms of the tabula recta. The tabula recta (from Latin *tabula rēcta*) is a square table of alphabets, each row of which is made by shifting the previous one to the left. The term was invented by the German author and monk Johannes Trithemius in 1508. It uses a letter square with the 26 letters of the alphabet following 26 rows of additional letters, each shifted once to the left. This creates 26 different Caesar ciphers.

Ciphertext

Ciphertext is the result of encryption performed on plaintext using an algorithm, called a cipher. Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. Decryption, the inverse of encryption, is the process of turning ciphertext into readable plaintext. Ciphertext is not to be confused with code-text because the latter is a result of a code, not a cipher.

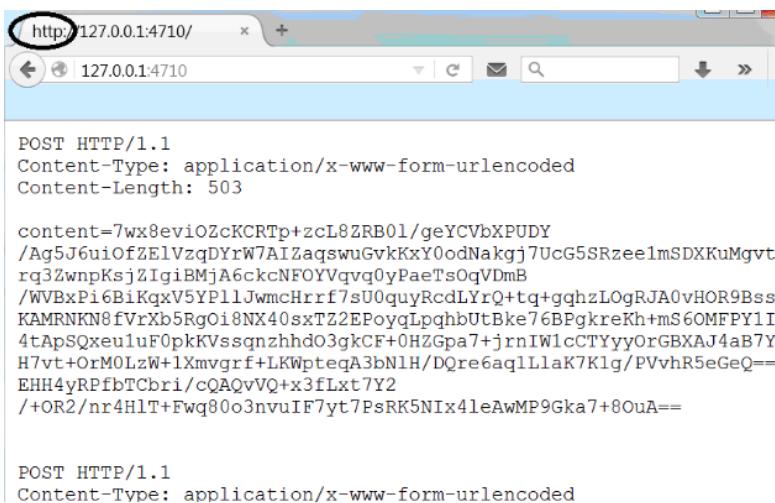


Figure 12: Ciphertext within a Web browser transferred to a HTTP Listener [PD]

Ciphertext posted to a HTTP Listener of the Application GoldBug Messenger captured within a Web browser by Adams/Maier 2016.

Ciphertext Stealing

Ciphertext stealing is a technique for encrypting plaintext using a block cipher, without padding the message to a multiple of the block size, so the ciphertext is the same size as the plaintext. It does this by altering processing of the last two blocks of the message. The processing of all but the last two blocks is unchanged, but a portion of the second-last block's ciphertext is "stolen" to pad the last plaintext block. The padded final block is then encrypted as usual. The final ciphertext, for the last two blocks, consists of the partial penultimate block (with the "stolen" portion omitted) plus the full final block, which are the same size as the original plaintext. Decryption requires decrypting the final block first, then restoring the stolen ciphertext to the penultimate block, which can then be decrypted as usual. In principle any block-oriented block cipher mode of operation can be used, but stream-cipher-like modes can already be applied to messages of arbitrary length without padding, so they do not benefit from this technique.

Clientside Encryption

Client-side encryption is the cryptographic technique of encrypting data before it is transmitted to a server in a computer network. Usually, encryption is performed with a key that is not known to the server. Consequently, the service provider is unable to decrypt the hosted data. In order to access the data, it must always be decrypted by the client. Client-side encryption allows for the creation of zero knowledge applications whose providers cannot

access the data its users have stored, thus offering a high level of privacy.

C-Mail

C-mail as a term describing e-mail, that is encrypted. This term was introduced (within the media reporting on the Snowden-papers on global surveillance) due to the awareness, that each e-mail is distributed over Internet servers readable like a postcard to any admin.

Collision Attack

A collision attack on a cryptographic hash tries to find two inputs producing the same hash value, i.e. a hash collision. This is in contrast to a preimage attack where a specific target hash value is specified. There are roughly two types of collision attacks:

Collision attack: Find two different messages m_1 and m_2 such that $\text{hash}(m_1) = \text{hash}(m_2)$.

More generally - Chosen-prefix collision attack: Given two different prefixes p_1 and p_2 , find two appendages m_1 and m_2 such that $\text{hash}(p_1 \parallel m_1) = \text{hash}(p_2 \parallel m_2)$, where \parallel denotes the concatenation operation.

Complexity

Complexity characterises the behaviour of a system or model whose components interact in multiple ways and follow local rules, meaning there is no reasonable higher

instruction to define the various possible interactions. The term is generally used to characterize something with many parts where those parts interact with each other in multiple ways, culminating in a higher order of emergence greater than the sum of its parts. The study of these complex linkages at various scales is the main goal of complex systems theory. A complex system is a system composed of many components which may interact with each other. Examples of complex systems are Earth's global climate, organisms, the human brain, infrastructure such as power grid, transportation or communication systems, social and economic organizations (like cities), an ecosystem, a living cell, and ultimately the entire universe. Complex systems are systems whose behavior is intrinsically difficult to model due to the dependencies, competitions, relationships, or other types of interactions between their parts or between a given system and its environment. Systems that are "complex" have distinct properties that arise from these relationships, such as nonlinearity, emergence, spontaneous order, adaptation, and feedback loops, among others. Because such systems appear in a wide variety of fields, the commonalities among them have become the topic of their own independent area of research. In many cases it is useful to represent such a system as a network where the nodes represent the components and the links their interactions. Computational complexity theory focuses on classifying computational problems according to their inherent difficulty, and relating these classes to each other. A computational problem is a task solved by a computer. A computation problem is solvable by mechanical application of mathematical steps,

such as an algorithm. A problem is regarded as inherently difficult if its solution requires significant resources, whatever the algorithm used. The theory formalizes this intuition, by introducing mathematical models of computation to study these problems and quantifying their computational complexity, i.e., the amount of resources needed to solve them, such as time and storage. Other measures of complexity are also used, such as the amount of communication (used in communication complexity), the number of gates in a circuit (used in circuit complexity) and the number of processors (used in parallel computing). One of the roles of computational complexity theory is to determine the practical limits on what computers can and cannot do. Closely related fields in theoretical computer science are analysis of algorithms and computability theory. A key distinction between analysis of algorithms and computational complexity theory is that the former is devoted to analyzing the amount of resources needed by a particular algorithm to solve a problem, whereas the latter asks a more general question about all possible algorithms that could be used to solve the same problem. More precisely, computational complexity theory tries to classify problems that can or cannot be solved with appropriately restricted resources. In turn, imposing restrictions on the available resources is what distinguishes computational complexity from computability theory: the latter theory asks what kind of problems can, in principle, be solved algorithmically.

Confidentiality

Confidentiality describes a property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Configuration

Configuration is related to security configurations of servers, devices, or software.

Congestion Control

Congestion control concerns controlling traffic entry into a telecommunications network, so as to avoid congestive collapse by attempting to avoid oversubscription of any of the processing or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets.

Continuous Improvement

A continuous improvement process is an ongoing effort to improve products, services, or processes. These efforts can seek "incremental" improvement over time or "breakthrough" improvement all at once. Delivery (customer valued) processes are constantly evaluated and improved in the light of their efficiency, effectiveness and flexibility. Some see CIPs as a meta-process for most management systems (such as business process

management, quality management, project management, and program management). The fact that it can be called a management process does not mean that it needs to be executed by 'management'; but rather merely that it makes decisions about the implementation of the delivery process and the design of the delivery process itself.

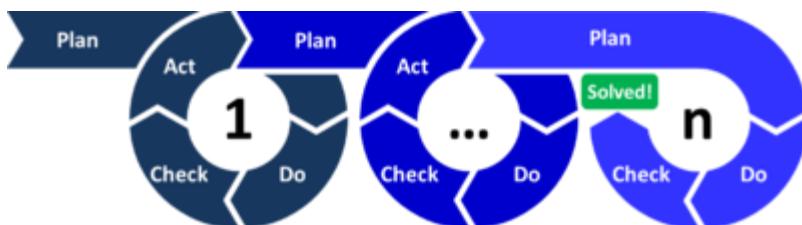


Figure 13: The PDCA-Cycle: Plan-Do-Check-Act [SA4]

Multiple iterations of the PDCA cycle are repeated until the problem is solved.

A broader definition is that of the Institute of Quality Assurance who defined "continuous improvement as a gradual never-ending change which is: ... focused on increasing the effectiveness and/or efficiency of an organisation to fulfil its policy and objectives. It is not limited to quality initiatives. Improvement in business strategy, business results, customer, employee and supplier relationships can be subject to continual improvement. Put simply, it means 'getting better all the time'. PDCA (plan-do-check-act or plan-do-check-adjust) is hereby an iterative four-step management method used in business for the control and continuous improvement of processes and products, which is also often referred to software

development, especially to find out weaknesses in cryptographic software for encryption.

Corrective Action

Corrective action is an action to eliminate the cause of a nonconformity and to prevent recurrence.

Crawler

A web crawler, sometimes called a spider or spiderbot and often shortened to crawler, is an Internet bot that systematically browses the World Wide Web, typically for the purpose of Web indexing (web spidering). Web search engines and some other sites use Web crawling or spidering software to update their web content or indices of other sites' web content. Web crawlers copy pages for processing by a search engine which indexes the downloaded pages so users can search more efficiently. Open source web crawlers are e.g. Grub, Nutch, Pandamonium (written in C++/Qt) or YaCy (for Java).

Credential

A credential is an attestation of qualification, competence, or authority issued to an individual by a third party with a relevant or de facto authority or assumed competence to do so. Examples of credentials include academic diplomas, academic degrees, certifications, security clearances, identification documents, badges, passwords, usernames,

keys, powers of attorney, and so on. Sometimes publications, such as scientific papers or books, may be viewed as similar to credentials by some people. Credentials in cryptography establish the identity of a party to communication. Usually they take the form of machine-readable cryptographic keys and/or passwords. Cryptographic credentials may be self-issued, or issued by a trusted third party; in many cases the only criterion for issuance is unambiguous association of the credential with a specific, real individual or other entity. Cryptographic credentials are often designed to expire after a certain period, although this is not mandatory. An x.509 certificate is an example of a cryptographic credential.

Cryptanalysis

Cryptanalysis (from the Greek *kryptós*, "hidden", and *analýein*, "to loosen" or "to untie") is the study of analyzing information systems in order to study the hidden aspects of the systems. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown. In addition to mathematical analysis of cryptographic algorithms, cryptanalysis includes the study of side-channel attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their implementation. Even though the goal has been the same, the methods and techniques of cryptanalysis have changed drastically through the history of cryptography, adapting to increasing cryptographic complexity, ranging from the pen-and-paper

methods of the past, through machines like the British Bombes and Colossus computers at Bletchley Park in World War II, to the mathematically advanced computerized schemes of the present. Methods for breaking modern cryptosystems often involve solving carefully constructed problems in pure mathematics, the best-known being integer factorization. Given some encrypted data ("ciphertext"), the goal of the cryptanalyst is to gain as much information as possible about the original, unencrypted data ("plaintext"). It is useful to consider two aspects of achieving this. The first is breaking the system — that is discovering how the encipherment process works. The second is solving the key that is unique for a particular encrypted message or group of messages. Asymmetric cryptography (or public key cryptography) is cryptography that relies on using two (mathematically related) keys; one private, and one public. Such ciphers invariably rely on "hard" mathematical problems as the basis of their security, so an obvious point of attack is to develop methods for solving the problem. The security of two-key cryptography depends on mathematical questions in a way that single-key cryptography generally does not, and conversely links cryptanalysis to wider mathematical research in a new way. Asymmetric schemes are designed around the (conjectured) difficulty of solving various mathematical problems. If an improved algorithm can be found to solve the problem, then the system is weakened. Another distinguishing feature of asymmetric schemes is that, unlike attacks on symmetric cryptosystems, any cryptanalysis has the opportunity to make use of knowledge gained from the public key. For symmetric

cryptography a brute-force attack is the most known cryptanalysis method and it consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

Crypto-Agility

Crypto-agility ('cryptographic agility') is the characteristic of an information security system to quickly switch to an alternative cryptographic primitives and algorithms without making significant changes to the systems infrastructure. Crypto-agility facilitates and encourages system upgrades and evolution. Crypto-agility can also act as a safety measure or an incident response mechanism when the essential encryption algorithms of a system are discovered to be weak or vulnerable. A security system is considered crypto-agile if the implementation of better encryption algorithms can be done with ease and is at least partly automated.

Cryptogram

A cryptogram is a type of puzzle that consists of a short piece of encrypted text. Generally the cipher used to encrypt the text is simple enough that the cryptogram can be solved by hand. Frequently used are substitution ciphers where each letter is replaced by a different letter or number. To solve the puzzle, one must recover the original lettering. Though once used in more serious applications,

they are now mainly printed for entertainment in newspapers and magazines.

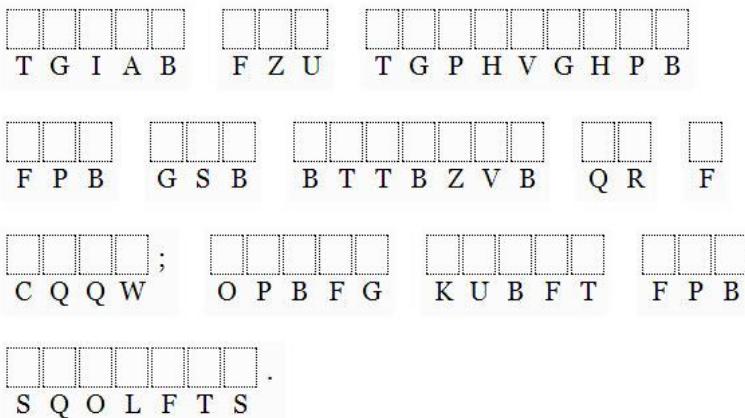


Figure 14: Example of a cryptogram [CC3]

Example cryptogram. When decoded it reads: "Style and structure are the essence of a book; great ideas are hogwash." -Vladimir Nabokov

Cryptographic Calling

Cryptographic Calling is a way to provide end-to-end credentials over a secure connection. The temporary key can be a-symmetric (PKI) or symmetric (a password string also known as a passphrase). The idea is to make end-to-end encryption as easy as calling a partner over a phone, just taking the phone, call, and if the session has to end, to change the temporary keys again and quit the call. Hence, a "Call" transfers over a public/private key encrypted environment a symmetric key (e.g. AES). It is a password for the session talk, only the two participants know.

Criteria	Asymmetric Calling	Forward Secrecy Calling	Symmetric Calling	SMP Calling	Secret Streams	Fiasco Forwarding	2-Way Calling
TLS/SSL-Connection	YES	YES	YES	YES	YES	YES	YES
Permanent asymmetric Chat/E-Mail Key	YES	YES	YES	YES	YES	YES	YES
Symmetric AES as Gemini	NO	NO	YES	NO	NO	NO	NO
Half AES + Half AES	NO	NO	NO	NO	NO	NO	YES
Secret SMP Password	NO	NO	NO	YES	YES	NO	NO
Ephemeral/temp. Chat/E-Mail PKI-Key	NO	YES	NO	NO	NO	NO	NO
Forward Secrecy as Pre-Condition	NO	YES	YES	NO	NO	YES	NO
Instant Perfect Forward Secrecy as result	YES	YES	YES	YES	YES	YES	YES
Several keys as a result	NO	NO	NO	NO	YES	YES	NO

Figure 15: Overview of the different types of Cryptographic Calling with respective criteria by Scott Edwards [PD]

With one click the user can instantly renew the end-to-end encryption password for the talk, respective text chat. It is also possible to manually define the end-to-end encrypted password (manually defined Calling). There are five further different ways to call: Asymmetric Calling, Forward Secrecy Calling, Symmetric Calling, SMP-Calling and 2-Way-Calling. The term of a “Call” in Cryptography has been introduced by Spot-on Encryption Suite, the integrated library and kernel of the Spot-On Application, and refers to sending a new end-to-end encryption password to the other participant.

Cryptographic Discovery

Cryptographic Discovery describes the method of an Echoing Protocol to find nodes in an Echo Network. Peers are aware of other peers and their cryptographic identities based on a cryptographic discovery within the network. Nodes inform other nodes about their neighbors, so that they can be addressed. Cryptographic discovery is then a mechanism which allows servers to lighten the computational and data responsibilities of e.g. mobile devices. It is implemented in the Messenger Smoke and its server software SmokeStack. Shortly after a Smoke instance connects to a SmokeStack service, the Smoke instance shares some nonprivate material. The material allows a SmokeStack server to transfer messages to their correct destinations. To mitigate replay attacks, Smoke offers SmokeStack instances random identity streams during message-retrieval requests. The identity streams self-expire. Nodes are sprinkled with routing information.

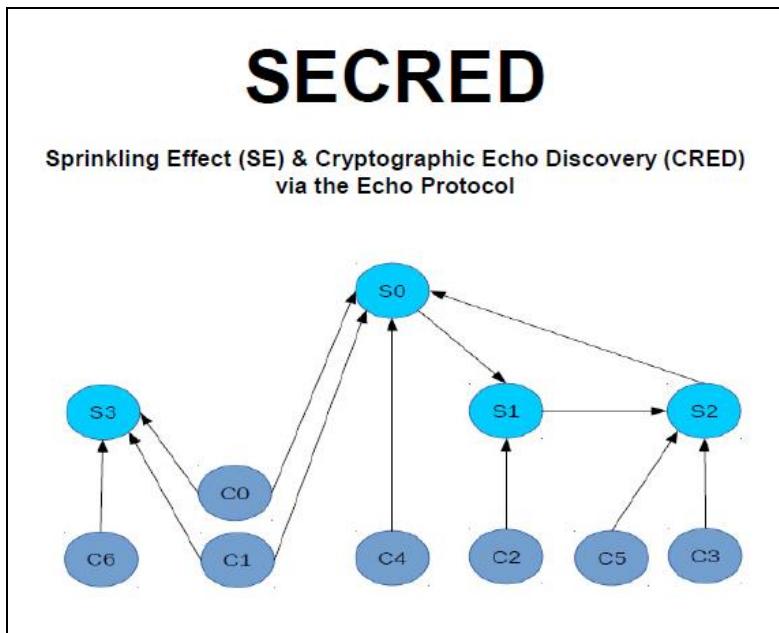


Figure 16: The Sprinkling Effect of SECRED within Cryptographic Discovery [PD]

Description of the sprinkling effect based on the Spot-On Project Documentation (07/2016) summarized by Gasakis / Schmidt (2018).

Cryptographic DNA

Cryptographic DNA is derived as term - in allusion to the DNA term taken from biology - from Magnet-URI-Links containing an assortment of specific cryptographic values. These values describe key size, algorithm, hash, iteration count etc. As each link can be different, the term DNA describes the specific uniqueness or footprint of such a bundle.

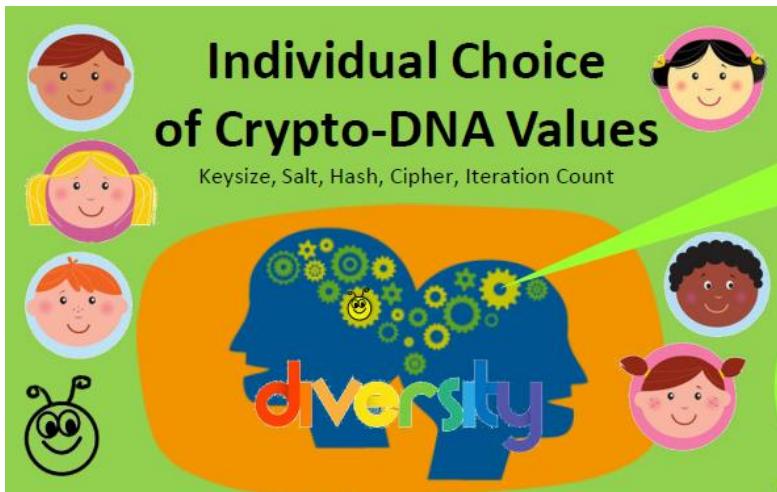


Figure 17: Diversity approach for cryptographic DNA values [PD]

Illustration of the Diversity approach by Adams/Maier (2016) in choosing cryptographic DNA values in creating encryption.

Cryptographic Protocol

A security protocol (cryptographic protocol or encryption protocol) is an abstract or concrete protocol that performs a security-related function and applies cryptographic methods, often as sequences of cryptographic primitives. A protocol describes how the algorithms should be used. A sufficiently detailed protocol includes details about data structures and representations, at which point it can be used to implement multiple, interoperable versions of a program. Cryptographic protocols are widely used for secure application-level data transport. A cryptographic protocol usually incorporates at least some of these

aspects: Key agreement or establishment, Entity authentication, Symmetric encryption and message authentication material construction, Secured application-level data transport, Non-repudiation methods, Secret sharing methods, Secure multi-party computation. For example, Transport Layer Security (TLS) is a cryptographic protocol that is used to secure web (HTTP/HTTPS) connections. It has an entity authentication mechanism, based on the X.509 system; a key setup phase, where a symmetric encryption key is formed by employing public-key cryptography; and an application-level data transport function. These three aspects have important interconnections. Standard TLS does not have non-repudiation support. There are other types of cryptographic protocols as well, and even the term itself has various readings; Cryptographic application protocols often use one or more underlying key agreement methods, which are also sometimes themselves referred to as "cryptographic protocols".

Cryptographic Routing

Cryptographic Routing is a term, which has been used as an antagonism for describing the Echo Protocol, as this is: beyond Routing. Echo means forwarding a message, which is address-less. So, no routing is given within Echo. A Cryptographic Routing would be given, if a node would have a certain Cryptographic Token as identifier. This is the case within Adaptive Echo (AE). Here in partial one can speak of cryptographic routing, as a target address might be given.

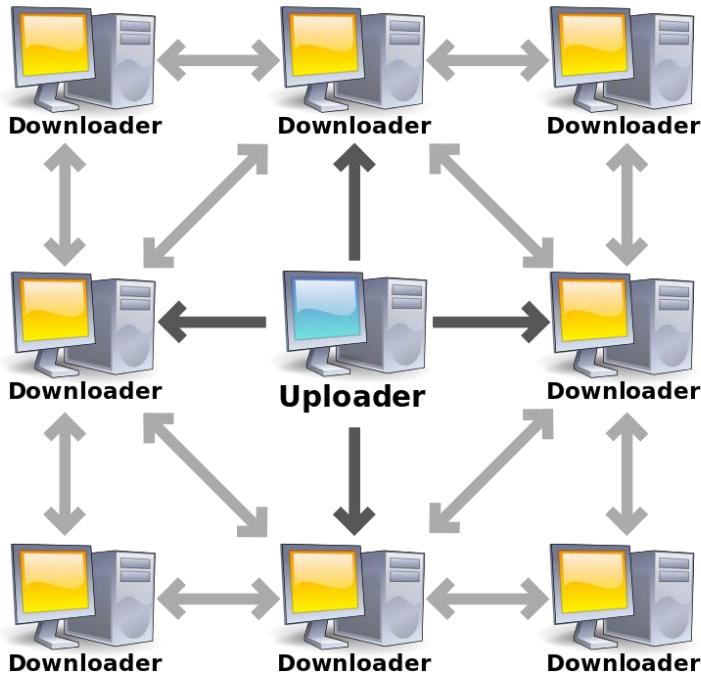


Figure 18: Cryptographic torrents [SA3]

The middle computer is acting as a "seed" to provide a file to the other computers which act as peers. Cryptographic Torrents are given, if each sent packet is encrypted and each computer sends to each connected neighbor.

Cryptographic Torrents

Cryptographic Torrents are defined by a bunch of cryptographic values, listed in a link to generate a download of a file. Similar to Torrent Links the download is started packet by packet, just with the difference that all

packets are encrypted, and the link contains an assortment of cryptographic values.

Cryptography & Cryptology

Cryptography (from Ancient Greek: κρυπτός, translit. kryptós "hidden, secret"; and γράφειν graphein, "to write", or -λογία -logia, "study", respectively) is the practice of techniques for secure communication in the presence of third parties called adversaries. Cryptology is the study of these techniques. The first use of the term cryptograph (as opposed to cryptogram) dates back to the 19th century—originating from The Gold-Bug, a novel by Edgar Allan Poe. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shares the decoding technique only with intended recipients to preclude access from adversaries. The cryptography literature often uses the names Alice ("A") for

the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary. Since the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptology have become increasingly complex and its application more widespread. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to use in practice than the best theoretically breakable but computationally secure mechanisms. Cryptography also plays a major role in digital rights management and copyright infringement of digital media.

CryptoPad

A Cryptopad is a tool, to convert plaintext to cipher text. A first suite integrated Pad has been developed by the Spot-On application under the name Rosetta-CryptoPad. The name derives from the Stone of Rosette in the Museum of

London, which is an index to read hieroglyphs. The Rosetta-CryptoPad uses asymmetric keys, so it is based on PKI and both participants need to share (and enter) the public key. It is not based on symmetric keys, with which the other user just has to enter a passphrase-string, e.g. known from encrypted PDF files.

Crypto-Parties

A Crypto-Party is a grassroots global endeavour to introduce the basics of practical cryptography such as software testing, creating different anonymity networks, key signing parties, disk encryption and virtual private networks to the general public. The project primarily consists of a series of free public workshops. Marcin de Kaminski, founding member of Piratbyrån which in turn founded The Pirate Bay, regards CryptoParty as the most important civic project in cryptography today, and Cory Doctorow has characterized a CryptoParty as being "like a Tupperware party for learning crypto." Der Spiegel in December 2014 mentioned "crypto parties" in the wake of the Edward Snowden leaks in an article about the NSA.



Figure 19: A flyer for a CryptoParty [CC3]

A flyer for a CryptoParty in Santiago, Chile, featuring Alice in Wonderland imagery.

CrypTool

CrypTool is an open-source project. The main result is the free e-learning software CrypTool illustrating cryptographic and cryptanalytic concepts. CrypTool implements more than 400 algorithms. Users can adjust these with own parameters. The graphical interface, online documentation, analytic tools and algorithms of CrypTool introduce users to the field of cryptography. CrypTool contains most classical ciphers, as well as modern symmetric and asymmetric cryptography including RSA, ECC, digital signatures, hybrid encryption, homomorphic encryption, and Diffie-Hellman

key exchange. Methods from the area of quantum cryptography (like BB84 key exchange protocol) and the area of post-quantum cryptography (like McEliece, WOTS, Merkle-Signature-Scheme, XMSS, XMSS_MT, and SPHINCS) are implemented. Many methods (for instance Huffman code, AES, Keccak, MSS) are visualized. CrypTool is worldwide the most widespread e-learning software in the field of cryptology. In addition, it contains: didactical games (like Number Shark, Divider Game, or Zudo-Ku) and interactive tutorials about primes, elementary number theory, and lattice-based cryptography. It is found under the Website www.cryptool.org

CSEK - Customer Supplied Encryption Keys

CSEK is the short abbreviation of Customer Supplied Encryption Keys. This refers to services, Internet offers and software architecture, which provides the option, that the user brings in his own keys, either symmetric or asymmetric. This is especially important for applications providing end to end encryption that users can insert or define their own password and use other channels to exchange the password. Customer Supplied Encryption Keys have been introduced as term by Google to provide customers to use own keys for the encryption of data within the Google cloud.

Data Exposure

Data exposure is related to unintended exposure of sensitive information.

Data Obfuscation

Data obfuscation or data masking is the process of hiding original data with modified content (characters or other data.) The main reason for applying masking to a data field is to protect data that is classified as personal identifiable data, personal sensitive data or commercially sensitive data, however the data must remain usable for the purposes of undertaking valid test cycles. It must also look real and appear consistent. In some organizations, data that appears on terminal screens to call centre operators may have masking dynamically applied based on user security permissions. (e.g.: Preventing call centre operators from viewing Credit Card Numbers in billing systems). The primary concern from a corporate governance perspective is that personnel conducting work in these non-production environments are not always security cleared to operate with the information contained in the production data. This practice represents a security hole where data can be copied by unauthorised personnel and security measures associated with standard production level controls can be easily bypassed. This represents an access point for a data security breach. Encryption is often a complex approach to solving the data masking problem. The encryption algorithm often requires that a "key" be applied to view the data based on user rights. This often sounds like the best

solution but in practice the key may then be given out to personnel without the proper rights to view the data and this then defeats the purpose of the masking exercise.

Data Validation

Data Validation is related to improper reliance on the structure or values of data.

Database Encryption

Database encryption can generally be defined as a process that uses an algorithm to transform data stored in a database into "cipher text" that is incomprehensible without first being decrypted. It can therefore be said that the purpose of database encryption is to protect the data stored in a database from being accessed by individuals with potentially "malicious" intentions. The act of encrypting a database also reduces the incentive for individuals to hack the aforementioned database as "meaningless" encrypted data is of little to no use for hackers. There are multiple techniques and technologies available for database encryption. *Symmetric database encryption:* Symmetric encryption in the context of database encryption involves a private key being applied to data that is stored and called from a database. This private key alters the data in a way that causes it to be unreadable without first being decrypted. Data is encrypted when saved, and decrypted when opened given that the user knows the private key. Thus if the data is to be shared through a database the receiving individual must have a

copy of the secret key used by the sender in order to decrypt and view the data. A clear disadvantage related to symmetric encryption is that sensitive data can be leaked if the private key is spread to individuals that should not have access to the data. However, given that only one key is involved in the encryption process it can generally be said that speed is an advantage of symmetric encryption.

Asymmetric database encryption: Asymmetric encryption expands on symmetric encryption by incorporating two different types of keys into the encryption method: private and public keys. A public key can be accessed by anyone and is unique to one user whereas a private key is a secret key that is unique to and only known by one user. In most scenarios the public key is the encryption key whereas the private key is the decryption key. As an example, if individual A would like to send a message to individual B using asymmetric encryption, he would encrypt the message using Individual B's public key and then send the encrypted version. Individual B would then be able to decrypt the message using his private key. Individual C would not be able to decrypt Individual A's message, as Individual C's private key is not the same as Individual B's private key. Asymmetric encryption is often described as being more secure in comparison to symmetric database encryption given that private keys do not need to be shared as two separate keys handle encryption and decryption processes.

Decentralized Computing

Decentralized computing is the allocation of resources, both hardware and software, to each individual workstation, or office location. Decentral means, there is no central server nor a web-interface to a central server. A client needs to be installed and adjusted locally on your device. Another term is: Distributed computing. Distributed computing is a field of computer science that studies distributed systems. A distributed system is a software system in which components located on networked computers communicate and coordinate their actions by passing messages. Based on a “grid model” a peer-to-peer system, or P2P system, is a collection of applications run on several local computers, which connect remotely to each other to complete a function or a task. There is no main operating system to which satellite systems are subordinate. This approach to software development (and distribution) affords developers great savings, as they don't have to create a central control point. An example application is LAN messaging which allows users to communicate without a central server.

Delta Chat

Delta.Chat is a Chat Messenger since late 2016 over e-mail servers implementing the prior released POPTASTIC (POP3/IMAP) Protocol idea (since 2014 released, see also Edwards, *ibid*): here over IMAP and OpenPGP. Delta Chat doesn't have their own servers but uses the most massive and diverse open messaging system ever: the existing e-

mail server network. That's POPTASTIC. Chat with anyone if one knows their e-mail address. All what is needed is a standard e-mail account. Delta Chat is an emerging chat app (since 2016, and since 2019 in beta status) that uses e-mails for transferring messages and encrypts the chat between two Delta-Chat installations. Key transport is done via the EPKS derivation Autocrypt. "Turtle File Sharing" Hopping as known from RetroShare over a friend-to-friend Web-of-Trust of e-mail-users as suggested by Gasakis/Schmidt (2018:67) under the concept of "POPTASTIC Echo Turtle" for an extension of the POPTASTIC Protocol respective an POPTASTIC Network is currently not yet implemented in Delta Chat; it would open up a secure file searching and sharing network over mobile devices between trusted friends the music/copyright-industry cannot influence as long as encryption and e-mail-servers exist for to be sent attachments (e.g. mp3s) over certain hops of a graph-route: e.g. a query-hit-sender and a searching receiver would share an ephemeral-temp public key over the POPTASTIC Protocol via E-Mail from friend to friend with some routing information and then wrap the MP3-file with their exchanged asymmetric encryption and send it over the same graph: Autocrypt-Transportation of the key and AutoSend-Transportation of the MP3-File from Queryhit-Node turtle-hopping over the e-mail-boxes of several friends to the searching friend. While utilizing a POPTASTIC Network for file sharing it must be spoken of routing, while utilizing an Echo Network (e.g. over the Mobile Crypto Chat App Smoke Messenger) it would be "beyond cryptographic routing" (*ibid*). Some e-mail-Providers like outlook.com, hotmail.com, office365.com

have not continued since 2019-02 to fix technical issues with Delta Chat (Issue #561). The hybrid implementation of additional private servers seems to be an adequate solution for that development of lacking support and limits of file sharing perspectives over e-mail servers at the same time.

Democratization of Encryption

Democratization of Encryption is a term coined by Scott Edwards (2019) within the title of the Handbook and Manual on the open source provision of the McEliece-Algorithm based Encryption Suite, which has been provided worldwide as first open source Desktop application for Messaging, E-Mailing and File-Sharing. The open source provision of quantum computing resistant algorithms within an applied programming for everyone to use founded a new cesura in cryptography.

Deniable Encryption

In cryptography and steganography, plausibly deniable encryption describes encryption techniques where the existence of an encrypted file or message is deniable in the sense that an adversary cannot prove that the plaintext data exists. The users may convincingly deny that a given piece of data is encrypted, or that they are able to decrypt a given piece of encrypted data, or that some specific encrypted data exists. Such denials may or may not be genuine. For example, it may be impossible to prove that the data is encrypted without the cooperation of the users. If the data is encrypted, the users genuinely may not be

able to decrypt it. Deniable encryption serves to undermine an attacker's confidence either that data is encrypted, or that the person in possession of it can decrypt it and provide the associated plaintext. Deniable encryption makes it impossible to prove the existence of the plaintext message without the proper decryption key. This may be done by allowing an encrypted message to be decrypted to different sensible plaintexts, depending on the key used. This allows the sender to have plausible deniability if compelled to give up his or her encryption key.

DFA - Differential Fault Analysis

Differential fault analysis (DFA) is a type of side channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults - unexpected environmental conditions - into cryptographic implementations, to reveal their internal states. For example, a smartcard containing an embedded processor might be subjected to high temperature, unsupported supply voltage or current, excessively high overclocking, strong electric or magnetic fields, or even ionizing radiation to influence the operation of the processor. The processor may begin to output incorrect results due to physical data corruption, which may help a cryptanalyst deduce the instructions that the processor is running, or what its internal data state is. For DES and Triple DES, about 200 single-flipped bits are necessary to obtain a secret key. Multi-Encryption - the conversion of ciphertext to ciphertext - might also reveal strengths and weaknesses to certain combined algorithms.

DHT - Distributed Hash Table

A Distributed Hash Table (DHT) is a class of a decentralized distributed system that provides a lookup service similar to a hash table: (key, value) pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key. Keys are unique identifiers which map to particular values, which in turn can be anything from addresses, to documents, to arbitrary data.

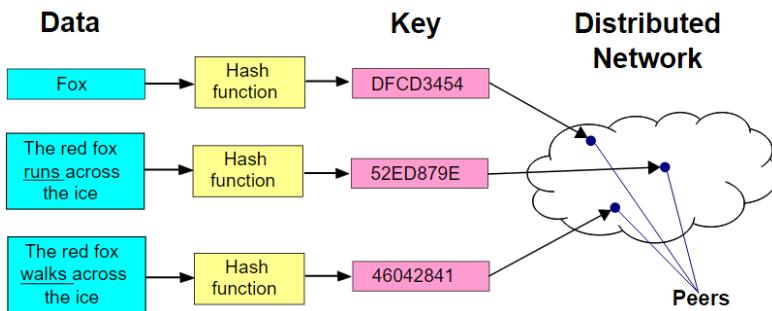


Figure 20: Distributed Hash Table (DHT) [PD]

A distributed hash table (DHT) is a class of a decentralized distributed system that provides a lookup service similar to a hash table: (key, value) pairs

Digest Access Authentication

Digest access authentication is one of the agreed-upon methods a web server can use to negotiate credentials, such as username or password, with a user's web browser. This can be used to confirm the identity of a user before sending sensitive information, such as online banking

transaction history. It applies a hash function to the username and password before sending them over the network. In contrast, basic access authentication uses the easily reversible Base64 encoding instead of encryption, making it non-secure unless used in conjunction with TLS. Technically, digest authentication is an application of MD5 cryptographic hashing with usage of nonce values to prevent replay attacks. It uses the HTTP protocol.

Digital Signature

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity). Digital signatures are a standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering. Digital signatures are often used to implement electronic signatures, which includes any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries electronic signatures have legal significance. Digital signatures employ asymmetric cryptography. In many instances they provide a layer of validation and security to messages sent through a non-secure channel: Properly implemented, a digital signature gives the receiver

reason to believe the message was sent by the claimed sender. Digital seals and signatures are equivalent to handwritten signatures and stamped seals. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret. Further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bitstring: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

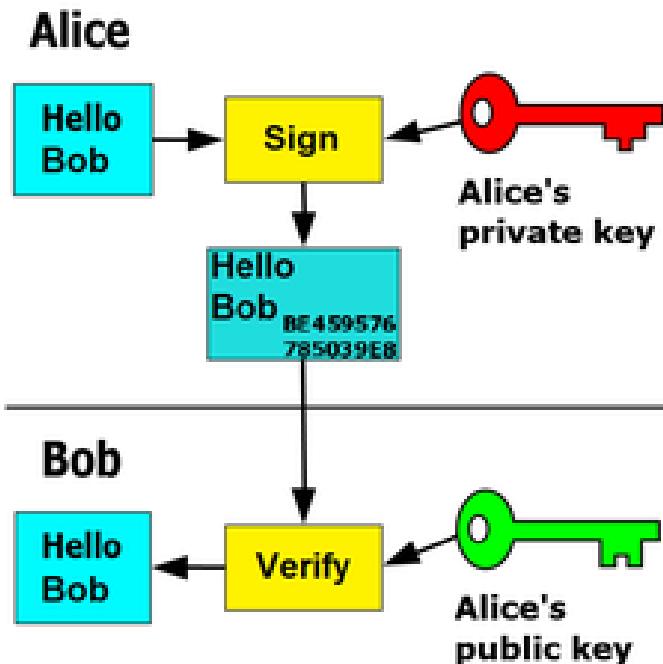


Figure 21: Digital Signature [PD]

In this example for a digital signature the message is only signed and not encrypted. 1) Alice signs a message with her private key. 2) Bob can verify that Alice sent the message and that the message has not been modified.

DNS - Domain Name System

The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain

names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System has been an essential component of the functionality of the Internet since 1985.

Documented Information

Documented information is information required to be controlled and maintained by an organization and the medium on which it is contained. Note: Documented information can be in any format and media and from any source.

Dooble Web Browser

Dooble is a free and open source Web browser. Dooble was created to improve privacy and provide an alternative in the sense of balance of power when the Google Chrome Browser was first time released. Currently, Dooble is available for FreeBSD, Linux, OS X, OS/2, and Windows. Dooble uses Qt for its user interface and abstraction from the operating system and processor architecture. As a result, Dooble should be portable to any system that supports OpenSSL, POSIX threads, Qt, SQLite, and other libraries.

DTLS - Datagram Transport Layer Security

Datagram Transport Layer Security (DTLS) is a communications protocol that provides security for datagram-based applications by allowing them to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the stream-oriented Transport Layer Security (TLS) protocol and is intended to provide similar security guarantees. The DTLS protocol datagram preserves the semantics of the underlying transport—the application does not suffer from the delays associated with stream protocols, but because it uses UDP, the application has to deal with packet reordering, loss of datagram and data larger than the size of a datagram network packet. Because DTLS uses UDP rather than TCP, it avoids the "TCP meltdown problem", when being used to create a VPN tunnel.

Eavesdropping

Eavesdropping is the act of secretly or stealthily listening to the private conversation or communications of others without their consent. The practice is widely regarded as unethical, and in many jurisdictions is illegal. The verb eavesdrop is a back-formation from the noun eavesdropper ("a person who eavesdrops"), which was formed from the related noun eavesdrop ("the dripping of water from the eaves of a house; the ground on which such water falls"). An eavesdropper was someone who would hang from the eave of a building so as to hear what is said within. The PBS

documentaries Inside the Court of Henry VIII (April 8, 2015) and Secrets of Henry VIII's Palace (June 30, 2013) include segments that display and discuss "eavedrops", carved wooden figures Henry VIII had built into the eaves (overhanging edges of the beams in the ceiling) of Hampton Court to discourage unwanted gossip or dissension from the King's wishes and rule, to foment paranoia and fear, and demonstrate that everything said there was being overheard; literally, that the walls had ears.



Figure 22: Cardinals eavesdropping in the Vatican [PD]

Kardinäle im Vorzimmer des Vatikans - A painting by Henri Adolphe Laissement, 1895.

Eavesdropping vectors include telephone lines, cellular networks, email, and other methods of private instant messaging; also speech recognition machines like Alexa, Siri, Ok-Google or Cortana can be used for it. VoIP

communications software is also vulnerable to electronic eavesdropping via infections such as trojans.

ECHELON

ECHELON, originally a secret government code name, is a surveillance program (signals intelligence/SIGINT collection and analysis network) operated by the US with the aid of four other signatory nations to the UKUSA Security Agreement: Australia, Canada, New Zealand and the United Kingdom, also known as the Five Eyes. The ECHELON program was created in the late 1960s to monitor the military and diplomatic communications of the Soviet Union and its Eastern Bloc allies during the Cold War, and it was formally established in 1971. By the end of the 20th century, the system referred to as "ECHELON" had evolved beyond its military and diplomatic origins to also become "...a global system for the interception of private and commercial communications" (mass surveillance and industrial espionage).



Figure 23: A radome to be used by ECHELON [PD]

A radome at RAF Menwith Hill, a site with satellite uplink capabilities believed to be used by ECHELON: The radome (which is a portmanteau of radar and dome) is a structural, weatherproof enclosure that protects a radar antenna. The radome is constructed of material that minimally attenuates the electromagnetic signal transmitted or received by the antenna, effectively transparent to radio waves. Radomes protect the antenna from weather and conceal antenna electronic equipment from view. They also protect nearby personnel from being accidentally struck by quickly rotating antennas.

Echo (Protocol)

Spot-On introduced the Echo - or: Echo-Protocol. The Echo is a malleable concept. That is, an implementation does not require rigid details. Each model may adhere to their own peculiar obligations. The Echo functions on the elementary persuasion that information is dispersed over multiple or singular passages and channel endpoints evaluate the suitability of the received data. Because data may become intolerable, Spot-On implements its own congestion control algorithm. Received messages that meet some basic criteria are labeled and duplicates are discarded. Advanced models may define more sophisticated congestion-avoidance algorithms based upon their interpretations of the Echo. The Echo combines encryption and graph theory: With the Echo Protocol is meant - simply put – that first, every message transmission is encrypted and second, in the Echo Network, each connection node sends each message to each connected neighbor. As third criterion for the Echo Protocol can be added, that there is a special feature when unpacking the encrypted capsule: The capsules have neither a receiver nor sender information included - and here they are different from TCP packets. The message is identified by the hash of the original message (compared to the conversion text of all known keys in the node) as to whether the message should be displayed and readable to the recipient in the user interface or not. For this so-called “Echo Match” see even more detailed at referring keyword. Spot-On Encryption Suite provides two modes of operation for the general Echo: Full Echo and Half Echo. The Full Echo permits absolute data flow. The Half Echo defines an agreement between two endpoints. Within this agreement,

information from other endpoints is prohibited from traveling along the private channel.

The Echo protocol means from an operational view: you send only encrypted messages, but you send your to-be-send-message to all of your connected friends. They do the same. You maintain your own network, everyone has every message and you try to decrypt every message. In case you can read and unwrap it, it is a message for you. Otherwise you share the message with all your friends and the message remains encrypted. Echo is very simple, and the principle is over 30 years old – nothing new: As Echo uses HTTP/S as a protocol, there is no forwarding or routing of messages: no IPs are forwarded, e.g. like it is if the user sends the own message e.g. from the home laptop to the own webserver. The process starts at each destination new – as the user defines it. The Echo protocol provided by the application Spot-On has nothing to do with RFC 862. A new Echo protocol RFC has to be written or re-newed and extended – with or without that RFC-Number it refers to a P2P or F2F network.

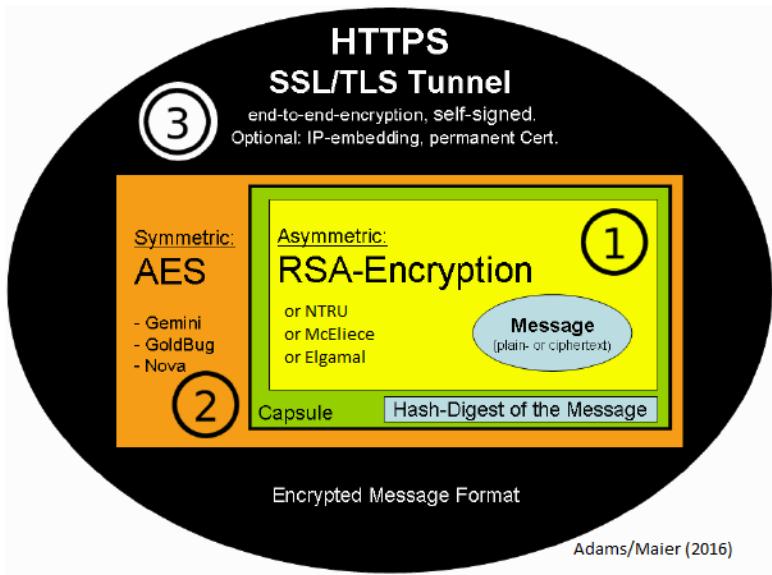


Figure 24: Graphical Scheme of three encryption layers for Multi-Encryption within the Echo-Protocol [PD]

(1) *First level of encryption: The message is encrypted, and the cipher text of the message is hashed and then the asymmetric key (e.g. with the RSA algorithm) can also be used to encrypt the symmetric keys. In an intermediate step, the encrypted text and the hash digest of the message are bundled into a capsule and packed together. It follows the paradigm: Encrypt-then-MAC. To prove to the recipient that the ciphertext has not been corrupted, the hash digest is first formed before the ciphertext is decrypted.*

(3) *Third level of encryption: Then this capsule can be transmitted via a secure SSL/TLS connection to the communication partner.*

(2) *Second level of encryption: Optionally, there is also the option of symmetrically encrypting the first-level capsule with an AES-256, which is comparable to a shared, 32-character password. Hybrid encryption is then added to multiple encryptions.*

Echo Accounts

Echo Accounts define an authorization scheme for the access to neighbor-nodes respective to the listener of a server. Within an Echo-Network a kind of firewall. At the same time, they can form a Web-of-Trust. One-Time-Accounts regulate the assignment of an access, which can be used one time.

Echo Match

The Echo Match is a specific cryptographic process to check the provided hash of the original message with the hash of the conversion of the ciphertext with a specific key. If both hashes are the same, the right key has been chosen. Because the hash function cannot be inverted, the provided hash of the original plaintext message does not provide any information about this message. Only if both hashes are the same, the conversion from cipher text to plaintext has been successful and the right user with the right key can read the message. This requires that each given key must be tried out and if the message cannot be converted successfully, that the message has to be provided to all known network connections and nodes to be tried out there: the message cannot be read by this node with given keys.

Practical Example and Process Description of the Echo-Match

Sender A hashed his original text to a hash 123456789, encrypts the text and packs the crypto-text and hash of the original message into the capsule (before he adds an AES-Password and sends it out via a TLS/SSL connection). Recipient 1 converts the received encoded text of the capsule to a (supposed) plaintext, but this has the hash 987654321 and is therefore not identical to the supplied original text hash of 123456789. This is repeated with all available keys of all friends of the recipient 1. Since all hash comparisons, however, were unsuccessful, he re-packs the message again and sends it on. The message is obviously not for him or from one of his friends. Recipient 2 now also converts the received, encrypted text to a (supposed) plaintext, this has the hash 123456789 and is thus identical to the supplied original text hash of 123456789, the decoding was apparently successful with one of the existing keys of his friends and therefore the message is displayed on the screen of this receiver.

Figure 25: Example for the Echo-Match (within a simplified process description).

Echo-Grid

The Echo-Grid is a graphical representation of a template for the Echo-protocol, do be able to illustrate different nodes and communicational relations in a graphic and within a view based on graph-theory. For that the letters for the word “E_C_H_O”, respective the both characters “A_E” for an Adaptive Echo Grid, are drawn and connected on a baseline. All angle corners of each letter further represent potential nodes in communicational networks, which can be per letter be consecutively numbered, example: E1 ... E1 for the six nodes of the letter E. Then it is

possible to talk about the communicational paths of drawn users from E to O.

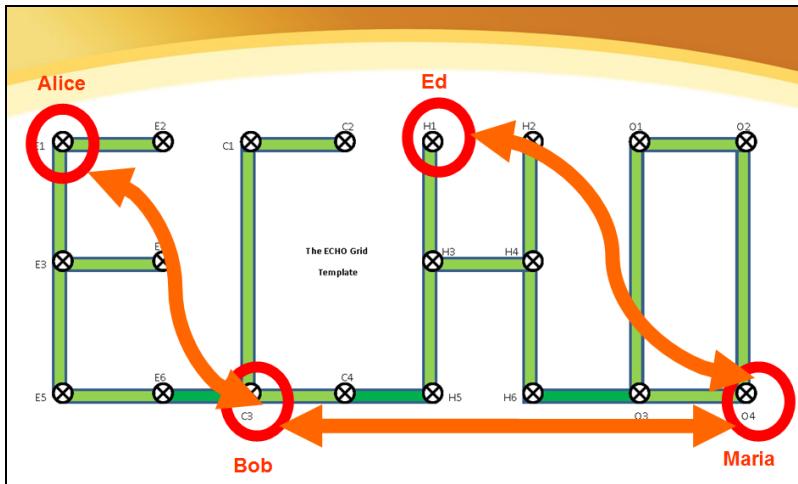


Figure 26: Example of a Grid-Template to explain networking [PD]

When talking about the Echo Protocol, often a simple Echo Grid template is drawn with the letters E_C_H_O. The nodes from E1 to O4 are numbered and connect the letters with a connecting line on the ground.

Echo-Network

The Echo-Network is a network based on Echo Nodes communicating over the Echo Protocol (and HTTPS). Often the letters E_C_H_O are used to provide a template for such a network within graph theory. The Echo network consists of servers and clients. Within the Spot-On clients the server software is already included, so that nodes can be in a hybrid position (so called: “Servent” – server and client at the same time), to be a server connected to a

server, a server connected to a node or a node connected to a server. The Echo Network is speaking of Neighbors for another node. An Echo Network is a kind of Mesh Network.

Edgar Allan Poe

Edgar Allan Poe (1809 – 1849) was an American writer, editor, and literary critic. Poe is best known for his poetry and short stories, particularly his tales of mystery and the macabre. He is widely regarded as a central figure of Romanticism in the United States and of American literature as a whole, and he was one of the country's earliest practitioners of the short story. One very popular short story was the story of "GoldBug". Hence, the software application also named GoldBug as an alternative GUI for the Spot-On kernel is a reminiscence to this writer. Poe is generally considered the inventor of the detective fiction genre and is further credited with contributing to the emerging genre of science fiction. He was the first well-known American writer to earn a living through writing alone, resulting in a financially difficult life and career. Poe was born in Boston and his works influenced literature around the world, as well as specialized fields such as cosmology and cryptography. He was a popular writer of cryptograms and interested in bringing the knowledge of cryptographic thinking to the population.

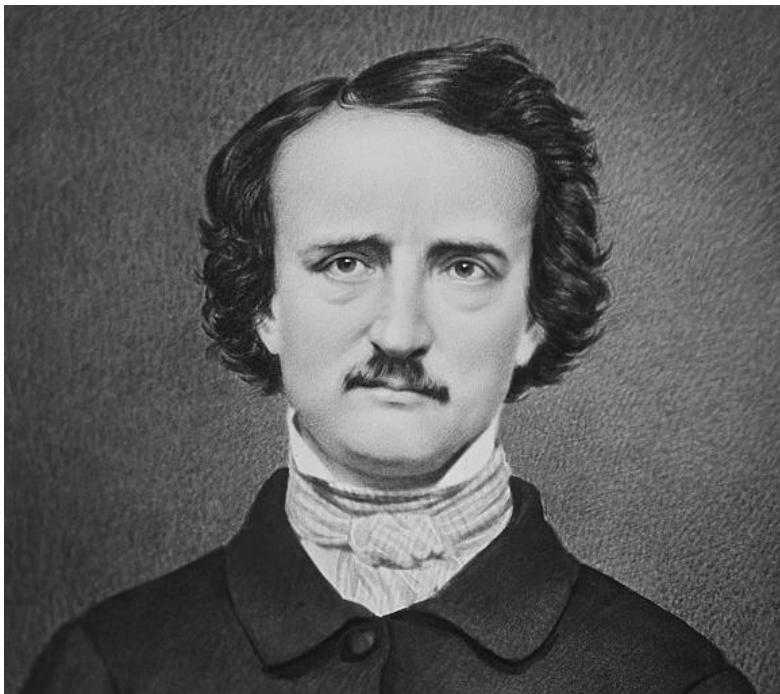


Figure 27: Edgar A. Poe [PD]

E-Government

E-Government (short for electronic government) is the use of electronic communications devices, such as computers and the Internet to provide public services to citizens and other persons in a country or region. According to Jeong, 2007 the term consists of the digital interactions between a citizen and their government (C2G), between governments and other government agencies (G2G), between government and citizens (G2C), between government and employees (G2E), and between government and

businesses/commerces (G2B). E-Government should enable anyone visiting a city website to communicate and interact with city employees via the Internet with graphical user interfaces (GUI), instant-messaging (IM), learn about government issues through audio/video presentations, and in any way more sophisticated than a simple email letter to the address provided at the site". The essence of e-governance is "The enhanced value for stakeholders through transformation" and "the use of technology to enhance the access to and delivery of government services to benefit citizens, business partners and employees". The focus should be on: The use of information and communication technologies, and particularly the Internet, as a tool to achieve better government. The use of information and communication technologies in all facets of the operations of a government organization. The continuous optimization of service delivery, constituency participation, and governance by transforming internal and external relationships through technology, the Internet and new media. Whilst e-government has traditionally been understood as being centered around the operations of government, e-governance is understood to extend the scope by including citizen engagement and participation in governance. As such, following in line with the OECD definition of e-government, e-governance can be defined as the use of ICTs as a tool to achieve better governance. Increased electronic contact and data exchange between government and its citizens goes both ways. Once E-Government technologies become more sophisticated, citizens will be likely be encouraged to interact electronically with the government for more transactions,

as e-services are much less costly than bricks and mortar service offices (physical buildings) staffed by civil servants. This could potentially lead to a decrease in privacy for civilians as the government obtains more and more information about their activities. Without safeguards, government agencies might share information on citizens. In a worst-case scenario, with so much information being passed electronically between government and civilians, a totalitarian-like system could develop. When the government has easy access to countless information on its citizens, personal privacy is lost.

ElGamal

In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key exchange. It was described by Taher ElGamal in 1985. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems.

Elliptic-Curve Cryptography

Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security. Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a

symmetric encryption scheme. They are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography, such as Lenstra elliptic-curve factorization. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible: this is the "elliptic curve discrete logarithm problem" (ECDLP). The security of elliptic curve cryptography depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the difficulty of the problem. The primary benefit promised by elliptic curve cryptography is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key: for example, a 256-bit elliptic curve public key should provide comparable security to a 3072-bit RSA public key. The U.S. National Institute of Standards and Technology (NIST) has endorsed elliptic curve cryptography in its Suite B set of recommended algorithms, specifically elliptic curve Diffie-Hellman (ECDH) for key exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signature. The U.S. National Security Agency (NSA) allows their use for protecting information classified up to top secret with 384-bit keys.

However, in August 2015, the NSA announced that it plans to replace Suite B with a new cipher suite due to concerns about quantum computing attacks on ECC.

E-Mail Institution

An E-Mail-Institution describes an E-Mail-Postbox within the P2P network of the Echo Protocol. Per definition of an address-like description for the institution, e-mails of users within the P2P network can temporarily be stored within one other node. As well it is possible, to send e-mail to friends, which are currently offline. Institutions describe a standard, how to configure an E-Mail-Postbox within a P2P network – like today POP3 and IMAP allow to provide a mailbox. The mailbox of the E-Mail-Institution is inserted by a Magnet-URI-Link within the client, which want to use the postbox. At the E-Mail-Institution only the public E-Mail-Encryption-Key of the postbox-users has to be entered.

Encapsulation

The capsule (like a zip) within the Echo describes a bundle of message elements, like the cipher text of the original message, the hash for the original message and also further elements like signature keys etc. In case an Echo Match was not successful, the elements of the capsule are encapsulated again and sent to further neighbors.

Encryption

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating ciphertext that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Enigma Machine

The Enigma machines are a series of electro-mechanical rotor cipher machines, mainly developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication. Enigma was invented by the German engineer Arthur Scherbius at the end of World War I. Early models were used commercially from the early 1920s, and adopted by military and government services of several countries. The German firm Scherbius & Ritter, co-founded by Arthur Scherbius,

patented ideas for a cipher machine in 1918 and began marketing the finished product under the brand name Enigma in 1923, initially targeted at commercial markets. With its adoption (in slightly modified form) by the German Navy in 1926 and the German Army and Air Force soon after, the name Enigma became widely known in military circles. The word enigma is a Latin word, derived from the Ancient Greek word enigma (ἀίγαλμα) used in English, but not native German. Like other rotor machines, the Enigma machine is a combination of mechanical and electrical subsystems. The mechanical subsystem consists of a keyboard; a set of rotating disks called rotors arranged adjacently along a spindle; one of various stepping components to turn at least one rotor with each key press, and a series of lamps, one for each letter. The mechanical parts act in such a way as to form a varying electrical circuit. When a key is pressed, one or more rotors rotate on the spindle. On the sides of the rotors are a series of electrical contacts that, after rotation, line up with contacts on the other rotors or fixed wiring on either end of the spindle. When the rotors are properly aligned, each key on the keyboard is connected to a unique electrical pathway through the series of contacts and internal wiring. Current, typically from a battery, flows through the pressed key, into the newly configured set of circuits and back out again, ultimately lighting one display lamp, which shows the output letter. For example, when encrypting a message starting ANX..., the operator would first press the A key, and the Z lamp might light, so Z would be the first letter of the ciphertext. The operator would next press N, and then X in the same fashion, and so on.



Figure 28: Rotors of the Enigma Machine [PD/CC1]

Enigma rotor assembly. In the Wehrmacht Enigma, the three installed movable rotors are sandwiched between two fixed wheels: the entry wheel, on the right, and the reflector on the left.

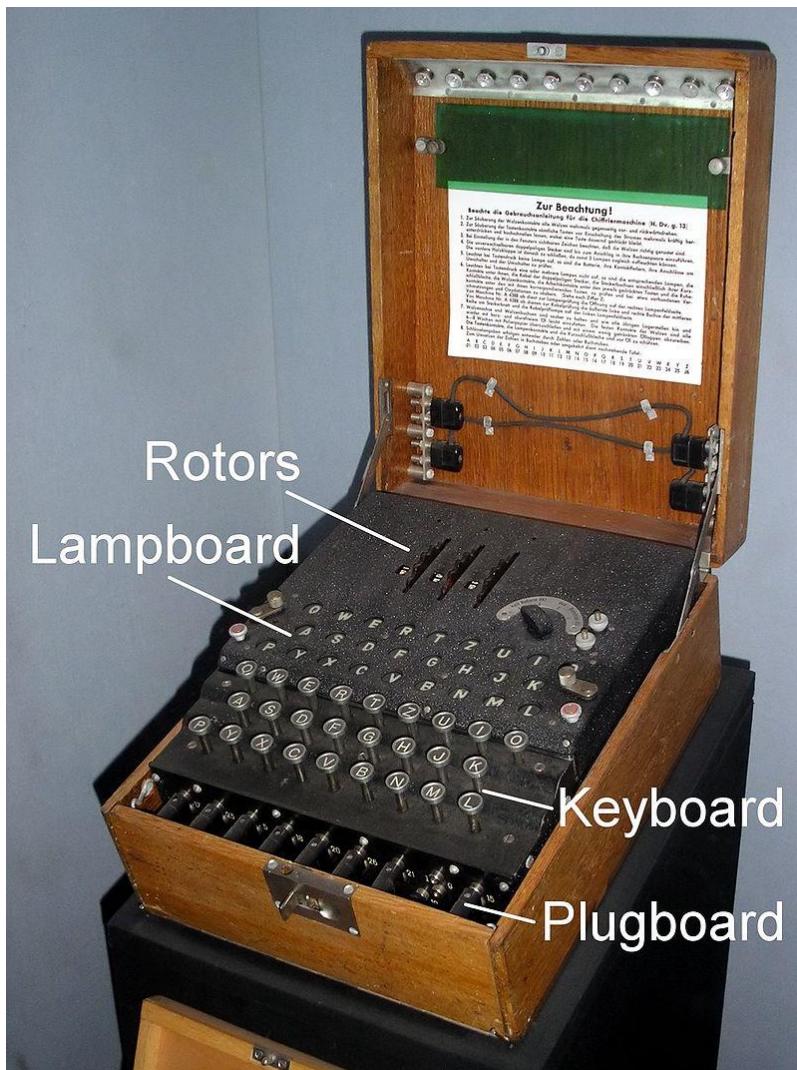


Figure 29: A three-rotor Enigma with plugboard [PD]

Entropy

Information entropy is the average rate at which information is produced by a stochastic source of data. The measure of information entropy associated with each possible data value is the negative logarithm of the probability mass function. When the data source produces a low-probability value (i.e., when a low-probability event occurs), the event carries more "information" ("surprisal") than when the source data produces a high-probability value. The amount of information conveyed by each event defined in this way becomes a random variable whose expected value is the information entropy. Generally, entropy refers to disorder or uncertainty, and the definition of entropy used in information theory is directly analogous to the definition used in statistical thermodynamics. The concept of information entropy was introduced by Claude Shannon in his 1948 paper "A Mathematical Theory of Communication".

Ephemeral & Session Keys

A session key is a single-use symmetric key used for encrypting all messages in one communication session. A closely related term is content encryption key (CEK), traffic encryption key (TEK), or multicast key which refers to any key used to encrypt messages, as opposed to other uses, like encrypting other keys (key encryption key (KEK) or key wrapping key). Session keys can introduce complication into a system. However, they solve some real problems. There are two primary reasons to use session keys: 1.

Several cryptanalytic attacks become easier as more material encrypted with a specific key is available. By limiting the amount of data processed using a particular key, those attacks are made more difficult. 2. Asymmetric encryption is too slow for many purposes, and all secret key algorithms require that the key is securely distributed. By using an asymmetric algorithm to encrypt the secret key for another, faster, symmetric algorithm, it's possible to improve overall performance considerably. This is the process used by PGP and GPG. Like all cryptographic keys, session keys must be chosen so that they cannot be predicted by an attacker, usually requiring them to be chosen randomly. Failure to choose session keys (or any key) properly is a major (and too common in actual practice) design flaw in any crypto system. A cryptographic key is called ephemeral if it is generated for each execution of a key establishment process. Ephemeral keys are temporarily used keys for encryption, often used for end-to-end encryption and/or to provide Forward Secrecy: Temporary keys are more deniable than permanent keys. In some cases ephemeral keys are used more than once, within a single session (e.g., in broadcast applications) where the sender generates only one ephemeral key pair per message and the private key is combined separately with each recipient's public key. Contrast with a static key. Private (resp. public) ephemeral key agreement keys are the private (resp. public) keys of asymmetric key pairs that are used a single key establishment transaction to establish one or more keys (e.g., key wrapping keys, data encryption keys, or MAC keys) and, optionally, other keying material (e.g., initialization vectors).

EPKS - Echo Public Key Share Protocol

Echo Public Key Share (EPKS) is a function implemented in Spot-On Encryption Suite to share public encryption keys over the Echo Network. This allows a group to share keys over secure channels so that a classical key server is not needed. It is a way of key exchange to a group or one individual user. The key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. If sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key. The key exchange problem is how to exchange whatever keys or other information are needed so that no one else can obtain a copy. Historically, this required trusted couriers, diplomatic bags, or some other secure channel. With the advent of public key / private key cipher algorithms, the encrypting key (aka public key) could be made public, since (at least for high quality algorithms) no one without the decrypting key (aka, the private key) could decrypt the message. Diffie-Hellman key exchange: In 1976, Whitfield Diffie and Martin Hellman published a cryptographic protocol, (Diffie-Hellman key exchange), which allows users to establish 'secure channels' on which

to exchange keys, even if an Opponent is monitoring that communication channel. However, D–H key exchange did not address the problem of being sure of the actual identity of the person (or ‘entity’). EPKS channels enable to exchange (symmetric and asymmetric) keys within a network as a broadcast without server storage. EPKS channels - and also BUZZ rooms - work on the same principle of symmetric encryption: The channel can be known to a community group or just one individual person.

ETM - Encrypt-then-MAC

The plaintext is first encrypted, then a MAC is produced based on the resulting ciphertext. The ciphertext and its MAC are sent together. Used in, e.g., Ipsec. The standard method according to ISO/IEC 19772:2009. This is the only method which can reach the highest definition of security in authenticated encryption, but this can only be achieved when the MAC used is “Strongly Unforgeable”. In November 2014, TLS and DTLS extension for Encrypt then Mac has been published as RFC 7366. Other approaches are Encrypt-and-MAC (E&M) and MAC-then-Encrypt (MtE).

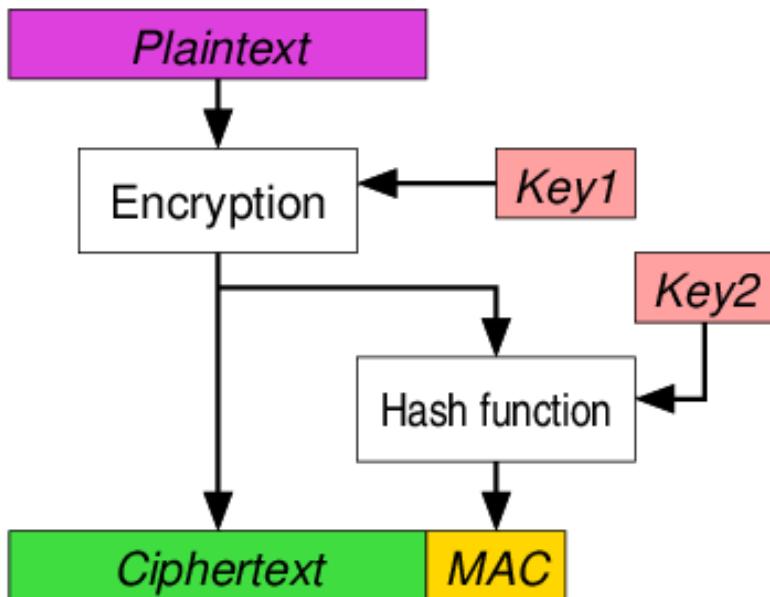


Figure 30: Authenticated encryption scheme "Encrypt Then Mac" (EtM) [PD]

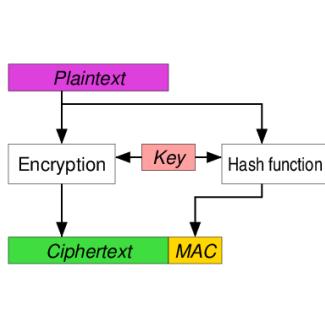


Figure 31: Authenticated encryption scheme "Encrypt and Mac" (E&M) [PD]

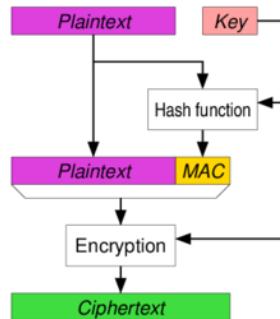


Figure 32: Authenticated encryption scheme "Mac then Encrypt" (MtE) [PD]

Exponential Encryption

Exponential Encryption is a term coined by the analysts and authors Meke Gasakis and Max Schmidt in their book about „The New Era of Exponential Encryption“ (EEE), in which they analyze based on the Echo Protocol the trends and their vision to provide exponential options for encryption and decryption processes in combination with graph-theory within Echo networks. Here each node sends each message to each known neighbor, which multiplicities the options like a rice corn – according to a popular story - doubling at each field of a chess board.

Exponential Encryption brings network theory including graph theory and encryption together and multiplies the options.

Also, a description of working together in community driven projects is described and the foundation of Cryptographic Discovery, the learning of machines/nodes by Cryptographic Tokens, has been founded within that book. Four arms of development are identified by the authors based on their analysis:

Metadata-Resistance: Avoidance of meta-data recording e.g. by usage of protocols minimizing this.

Multi-Encryption: Hybrid and/or Multi-Encryption means: Ciphertext is converted to ciphertext once more or several Algorithms are deployed.

Diversity of Crypto-DNA: Manual definition of parameters for individual encryption-options are enable for the user, e.g. by means of Cryptographic Calling or Instant Perfect Forward Secrecy (IPFS) or End-to-End encryption in general.

Quantum-Resistance: e.g. with NTRU and McEliece algorithms - Change of the algorithms for more security in spite of quantum computing.

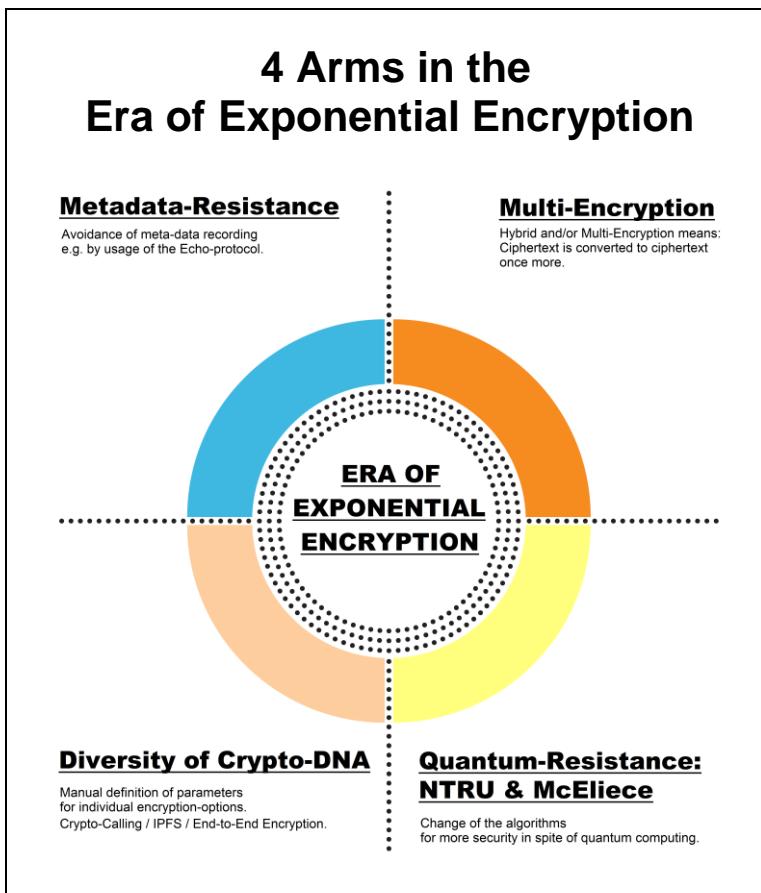


Figure 33: Four Arms in the Era of Exponential Encryption [PD]

Exponential Key Exchange

A key-agreement protocol is a protocol whereby two or more parties can agree on a key in such a way that both influence the outcome. If properly done, this precludes undesired third parties from forcing a key choice on the agreeing parties. Protocols that are useful in practice also do not reveal to any eavesdropping party what key has been agreed upon. An early publicly known public-key agreement protocol that meets the above idea was the Diffie-Hellman key exchange, in which two parties jointly *exponentiate* a generator with random numbers, in such a way that an eavesdropper cannot feasibly determine what the resultant value used to produce a shared key is. That referred to the number generator. Many key exchange systems have one party generate the key, and simply send that key to the other party -- the other party has no influence on the key. Using a key-agreement protocol avoids some of the key distribution problems associated with such systems. Also, Two-way Cryptographic Calling defines a key in agreement with the other party. *Exponential key exchange* in and of itself does not specify any prior agreement or subsequent authentication between the participants. It has thus been described as an anonymous key agreement protocol (compare authenticated key agreement, also including both parties, with Secret Stream Keys and/or Juggerknot Keys). A key agreement protocol in the direction of exponential key exchange are further Fiasco Keys, which send a bunch of keys for one message to be decrypted, hence it is not only a number generator, which defines an exponential key exchange, also several keys are exchanged. Key exchange

for a single key per session (like with OTR protocol) or a single key for each message (like with Signal protocol) found in Fiasco Keys an alternative, exchanging for each message a whole bunch of keys, in which two parties jointly not only exponentiate a generator with random numbers but also generate multiplied keys to be tried out for each sent message or packet. Within an Echo Network the key exchange and trying-out of keys starts towards exponential en-/decryption, as graph theory needs to be considered for this kind of Exponential Encryption. Exponential key exchange takes place in such a kind of flooding network.

E2EE - End-to-End Encryption

The end-to-end principle is a classic design principle of computer networking, first explicitly articulated in a 1981 conference paper by Saltzer, Reed, and Clark. The end-to-end principle states that application-specific functions ought to reside in the end hosts of a network rather than in intermediary nodes – provided they can be implemented “completely and correctly” in the end hosts. In debates about network neutrality, a common interpretation of the end-to-end principle is that it implies a neutral or “dumb” network. End-to-end encryption (E2EE) is an uninterrupted protection of the confidentiality and integrity of transmitted data by encoding it at its starting point and decoding it at its destination. It involves encrypting clear (red) data at source with knowledge of the intended recipient, allowing the encrypted (black) data to travel safely through vulnerable channels (e.g. public networks) to its recipient where it can be decrypted (assuming the

destination shares the necessary key-variables and algorithms). An end-to-end encryption is often reached by providing an encryption with AES or a Passphrase.

Facial Recognition System

A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from given image with faces within a database. It is also described as a Biometric Artificial Intelligence based application that can uniquely identify a person by analyzing patterns based on the person's facial textures and shape. While initially a form of computer application, it has seen wider uses in recent times on mobile platforms and in other forms of technology, such as robotics. It is typically used as access control in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. Although the accuracy of facial recognition system as a biometric technology is lower than iris recognition and fingerprint recognition, it is widely adopted due to its contactless and non-invasive process. Some applications include advanced human-computer interaction, video surveillance, automatic indexing of images, and video database, among others. Apple introduced Face ID on the flagship iPhone X as a biometric authentication successor to the Touch ID, a fingerprint-based system. Face ID has a facial recognition sensor that consists of two parts: a "Romeo" module that projects

more than 30,000 infrared dots onto the user's face, and a "Juliet" module that reads the pattern. The pattern is sent to a local "Secure Enclave" in the device's central processing unit (CPU) to confirm a match with the phone owner's face. Civil rights right organizations and privacy campaigners such as the Electronic Frontier Foundation, Big Brother Watch and the ACLU express concern that privacy is being compromised by the use of surveillance technologies. Some fear that it could lead to a "total surveillance society," with the government and other authorities having the ability to know the whereabouts and activities of all citizens around the clock. Face recognition can be used not just to identify an individual, but also to unearth other personal data associated with an individual – such as other photos featuring the individual, blog posts, social networking profiles, Internet behavior, travel patterns, etc. – all through facial features alone. Consumers may not understand or be aware of what their data is being used for, which denies them the ability to consent to how their personal information gets shared.

Fiasco Keys & Fiasco Forwarding

Fiasco Keys are temporary keys, which were first introduced within the Smoke Mobile Chat Client. These keys are a bunch of temporary keys provided in a cache for end to end encryption. Starting from the newest, all keys in that cache for Fiasco Forwarding have to be tried out. This is a more volatile construction than schematic key transmission known form other protocols. It has been implemented in the Smoke Mobile Encryption Messenger

as follows: Authentication and encryption key data which are established via the so-called Cryptographic Calling mechanism are recorded within the participants keys database table. Whenever a message from a SmokeStack instance (the referring server) is received, the message's digest is verified using each of the recorded authentication keys. Smoke iterates through the set of Fiasco authentication keys until a correct authentication key is discovered or the search is exhausted. If an authentication key is recovered, the message is deciphered and delivered locally. Newer authentication keys are tested first.

File-Encryptor

File-Encryptor is a tool within the Spot-On Encryption Suite to encrypt files before they are sent out over an encrypted or unencrypted connection or are stored within a cloud or a foreign storage option. The File Encryption Tool of Spot-On has the function to encrypt and decrypt files on the hard disk. Here as well many values for the encryption details can be set individually. The tool is useful, in case files have to be sent - either over encrypted or unencrypted connections to the internet. As well for the storage of files, either on the users local hard disc or as well remote in the cloud, this open source tool is very helpful, to secure own data.

File-Sharing

File sharing is the practice of distributing or providing access to digital media, such as computer programs,

multimedia (audio, images and video), documents or electronic books. File sharing may be achieved in a number of ways. Common methods of storage, transmission and dispersion include manual sharing utilizing removable media, (de-)centralized servers on computer networks, World Wide Web-based hyperlinked documents, and the use of (mobile) distributed peer-to-peer networking. As a peer could be an attacker today, a web-of-trust in a friend-to-friend-network has to be used to create a file sharing network. Servers are ideally e-mail servers (IMAP & POP3) over the encrypting POPTASTIC Protocol, which is additionally equipped with Turtle Hopping file sharing over the friends in the chain or graph to the sharing file source.

Fingerprint

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. The recovery of fingerprints from a crime scene is an important method of forensic science. Fingerprints are easily deposited on suitable surfaces (such as glass or metal or polished stone) by the natural secretions of sweat from the eccrine glands that are present in epidermal ridges. In public-key cryptography, a public key fingerprint is a short sequence of bytes used to identify a longer public key. Fingerprints are created by applying a cryptographic hash function to a public key. Since fingerprints are shorter than the keys they refer to, they can be used to simplify certain key management tasks. A public key fingerprint is typically created through the following steps: (1) A public key (and optionally some additional data) is encoded into a

sequence of bytes. To ensure that the same fingerprint can be recreated later, the encoding must be deterministic, and any additional data must be exchanged and stored alongside the public key. The additional data is typically information which anyone using the public key should be aware of. Examples of additional data include: which protocol versions the key should be used with (in the case of PGP fingerprints); and the name of the key holder (in the case of X.509 trust anchor fingerprints, where the additional data consists of an X.509 self-signed certificate).

(2) The data produced in the previous step is hashed with a cryptographic hash function such as SHA-1, SHA-2 or SHA-3.

(3) If desired, the hash function output can be truncated to provide a shorter, more convenient fingerprint. This process produces a short fingerprint which can be used to authenticate a much larger public key. For example, whereas a typical RSA public key will be 1024 bits in length or longer, typical MD5 or SHA-1 fingerprints are only 128 or 160 bits in length. When displayed for human inspection, fingerprints are usually encoded into hexadecimal strings.

FinSpy

FinSpy, also known as FinFisher, is surveillance software marketed by Lench IT Solutions plc, which markets the spyware through law enforcement channels. FinFisher can be covertly installed on targets' computers by exploiting security lapses in the update procedures of non-suspect software. The company has been criticized by human rights organizations for selling these capabilities to repressive or non-democratic states known for monitoring and

imprisoning political dissidents. Egyptian dissidents who ransacked the offices of Egypt's secret police following the overthrow of Egyptian President Hosni Mubarak reported that they had discovered a contract with Gamma International for €287,000 for a license to run the FinFisher software. In 2014, an American citizen sued the Ethiopian government for surreptitiously installing FinSpy onto his computer in America and using it to wiretap his private Skype calls and monitor his entire family's every use of the computer for a period of months. Lench IT Solutions plc has a UK-based branch, Gamma International Ltd in Andover, England, and a Germany-based branch, Gamma International GmbH in Munich. Gamma International is a subsidiary of the Gamma Group, specializing in surveillance and monitoring, including equipment, software, and training services. On August 6, 2014, FinFisher source code, pricing, support history, and other related data were retrieved from the Gamma International internal network and made available on the Internet. This hidden mobile application grabs entered text as plaintext before it is encrypted and sent. That's why "Going the Extra Mile" is important with typing on a device, that has never been connected to the Internet for updates ("Trusted Execution Environment"), and sends out the encrypted packet e.g. over a Bluetooth connection to another Internet connected device.

FireChat

FireChat is an IRC-like group chat within the Smoke Mobile Crypto Chat Client and compatible to the BUZZ-Chat in the

Spot-On Encryption Suite. The Fire chat activity is one of three messaging activities (next to PKI-based chat and 1:1 chat). From this activity, one may communicate with one or more groups of semi-anonymous participants. Fire is compatible with Spot-On's Buzz. 256-bit AESCBC along with SHA-384 HMAC provide the encryption and authentication.

Firewall

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines. The Great Firewall of China (GFW) is the combination of legislative actions and technologies enforced by the People's Republic of China to regulate the Internet domestically. Its role in the Internet censorship in China is to block access to selected foreign websites and to slow down cross-border internet traffic. The effect includes: limiting access to foreign information sources, blocking foreign internet tools (e.g. Google search, Facebook, Twitter etc.) and mobile apps, and requiring foreign companies to adapt to domestic regulations. Besides censorship, the GFW has also influenced the development of China's internal internet economy by nurturing domestic

companies and reducing the effectiveness of products from foreign internet companies.

Flooding

Flooding is used in computer networks routing algorithm in which every incoming packet is sent through every outgoing link except the one it arrived on. Flooding is used in bridging and in systems such as Usenet and peer-to-peer file sharing and as part of some routing protocols, e.g. the ECHO Protocol within a Mesh Network and other, including OSPF, DVMRP, and those used in ad-hoc wireless networks (WANETs). A flooding algorithm is an algorithm for distributing material to every part of a graph. The name derives from the concept of inundation by a flood. Flooding algorithms are used in computer networking and graphics. Flooding algorithms are also useful for solving many mathematical problems, including maze problems and many problems in graph theory. Today the term Mesh Network is more up to date than the term Flooding Network.

Forward Secrecy

Forward Secrecy (FS), also known as perfect forward secrecy (PFS), is a feature of specific key agreement protocols that gives assurances your session keys will not be compromised even if the private key of the server is compromised. Forward secrecy protects past sessions against future compromises of secret keys or passwords. By generating a unique session key for every session, a user

initiates, even the compromise of a single session key will not affect any data other than that exchanged in the specific session protected by that particular key. It has been enhanced to Instant Perfect Forward Secrecy (IPFS), see also IPFS, where session keys can be renewed instantly with Cryptographic Calling.

Forward-Secrecy-Calling

Forward-Secrecy-Calling is some modus for Cryptographic Calling, which sends temporary asymmetric keys for end-to-end encryption and is referred to Asymmetric Calling. It refers to send several asymmetric key (pairs) through one secured channel. The symmetric end-to-end encryption key is sent in the Forward Secrecy Calling (FSC) not over the permanent (a-symmetric) e.g. chat key or over the channel of an existing (symmetric) end-to-end encryption key, but by the new ephemeral, temporary and a-symmetric (e.g. chat) key. While sending an end-to-end encryption key over an existing end-to-end symmetric encrypted channel defines a "symmetric" "instant perfect forward secrecy", sending an end-to-end encrypting key over the ephemeral keys of the initiated "forward secrecy" (in e.g. the chat function) may be considered as an "a-symmetric" one of "Instant Perfect Forward Secrecy".

Freedom of Speech

Freedom of speech is a principle that supports the freedom of an individual or a community to articulate their opinions and ideas without fear of retaliation, censorship, or legal sanction. The term "freedom of expression" is sometimes

used synonymously but includes any act of seeking, receiving, and imparting information or ideas, regardless of the medium used. Freedom of expression is recognized as a human right under article 19 of the Universal Declaration of Human Rights (UDHR) and recognized in international human rights law in the International Covenant on Civil and Political Rights (ICCPR). Article 19 of the UDHR states that "everyone shall have the right to hold opinions without interference" and "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". The version of Article 19 in the ICCPR later amends this by stating that the exercise of these rights carries "special duties and responsibilities" and may "therefore be subject to certain restrictions" when necessary "[f]or respect of the rights or reputation of others" or "[f]or the protection of national security or of public order (order public), or of public health or morals". Freedom of speech and expression, therefore, may not be recognized as being absolute, and common limitations or boundaries to freedom of speech exist, especially in regard of the harm to others.

Figure 34: While Silence means Security – means Free Speech in Public (or Plain Text over the Internet) the opposite? [PD]

Women's Army Corps propaganda (1941–1945) associated national security with avoiding conversations about war work.



Freenet

Freenet is a peer-to-peer platform for censorship-resistant communication. It uses a decentralized distributed data store to keep and deliver information and has a suite of free software for publishing and communicating on the Web without fear of censorship. The distributed data store of Freenet is used by many third-party programs and plugins to provide microblogging and media sharing, anonymous and decentralised version tracking, blogging, a generic web of trust for decentralized spam resistance. Since version 0.7, Freenet offers two different levels of security: Opennet and Friendsnet. With Opennet, users connect to arbitrary other users. With Friendsnet, users connect only to "friends" with whom they previously exchanged public keys, named node-references. Both modes can be used together.

Full Echo

See Echo.

F2F - Friend-to-Friend

A friend-to-friend (or F2F) computer network is a type of peer-to-peer network in which users only make direct connections with people they know. Passwords or digital signatures can be used for authentication. Unlike other kinds of private P2P, users in a friend-to-friend network cannot find out who else is participating beyond their own

circle of friends, so F2F networks can grow in size without compromising their users' anonymity.

GCM - Galois/Counter Mode-Algorithm

Galois/Counter Mode (GCM) is a mode of operation for symmetric key cryptographic block ciphers that has been widely adopted because of its efficiency and performance. GCM throughput rates for state of the art, high speed communication channels can be achieved with reasonable hardware resources.

Gemini

The Gemini is a feature in Spot-On Encryption Suite and Secure Instant Messenger to add another security layer to the chat with an AES-Key respective passphrase for end-to-end encryption. Both sides (like twins) need to know the passphrase for the decryption and encryption process.



Figure 35: Gemini as term for twins representing a symmetric passphrase [PD]

Gemini as term for twins represent in cryptography a symmetric passphrase, known at both sides. Gemini is an astrological sign, originating from the constellation of Gemini. Under the tropical zodiac, the sun transits this sign between about May 21 and June 21. Gemini is represented by the twins Castor and Pollux. Image out of a medieval book of astrology (15th century).

GnuPG - GNU Privacy Guard

GNU Privacy Guard (GnuPG or GPG), a free-software replacement for Symantec's PGP cryptographic software suite, complies with RFC 4880, the IETF standards-track specification of OpenPGP. Modern versions of PGP are interoperable with GnuPG and other OpenPGP-compliant systems. GnuPG is a hybrid-encryption software program because it uses a combination of conventional symmetric-key cryptography for speed, and public-key cryptography for ease of secure key exchange, typically by using the recipient's public key to encrypt a session key which is only used once. GnuPG encrypts messages using asymmetric key pairs individually generated by GnuPG users. The resulting public keys may be exchanged with other users in a variety of ways. GnuPG also supports symmetric encryption algorithms. By default, GnuPG uses the CAST5 symmetrical algorithm.

Gnutella

Gnutella has been a large peer-to-peer network. It was the first decentralized peer-to-peer network of its kind, leading to other, later networks adopting the model.

Going the Extra Mile

Going the Extra Mile is a term coined by human right activists for the process of encrypting plaintext on machines and mobile devices, that have never been connected to the internet, so that key logging by the

operating system or the keyboard app or other unknown applications, like online injected governmental trojan horses, hence: fetching the plaintext before it is encrypted, does not work out on these trusted execution environments - because the machine was never connected to the internet, so that there is no chance by third party to install or use such spying tools. Some operating system venders have discovered this option already and provide the option to deactivate the operating system or even the hardware chips, in case they are not connected to an online line after a while. Going the Extra Mile means then to connect an offline device e.g. with a Bluetooth listener to another device (or to transfer the encrypted capsule with an USB-stick from the trusted, not-Internet-connected operating system to another Internet-connected machine). The encrypted packet is then sent from the device, which has never been connected to the internet by a dedicated connection, e.g. this Bluetooth connection, to the second device, which is connected to the internet (e.g. via Wifi or Lan) and then passes the encrypted packet along. This Extra Mile then does not allow to use or install online a tool for "Quellen-Telekommunikations-Überwachung" (TKÜ) - as it is named in German -, a tool for copying the entered plaintext on the device, on which it is typed in. Devices, on which plaintext is typed, should be secured by the Extra Mile, which means they should never be or ever have been connected directly to the internet. Only fresh and unconnected devices provide the security of a trusted execution environment, on which typed text is not fetched. The process would be - as said - the same, if an offline device is encrypting the text and then the encrypted

capsule is transferred via USB stick to the online machine and then there picked up. Entering text - before it will be encrypted - needs maiden-like devices, which have never been online and are free from Trojan Horses or online connections, which could potentially offer the risk of injections or unnoticed send-outs. Going this Extra Mile on trusted execution environments (TEE) is additional effort but keeps the creation of the encrypted capsule in a safe and separated (unwatched) process. Going the Extra Mile is necessary to circumvent Spyware and Trojan Horses like Pegasus (Israel) or the Remote Control System (Italy) or FinFisher (Germany) next to potential options the operating system suppliers and suppliers of non-open-source messaging apps provide to requesting parties.

Goldbug (E-Mail Password)

The Goldbug-feature is used in the integrated email client of the software clients GoldBug and Spot-On to add here as well an end-to-end AES Encryption layer – the Goldbug, or: just a password, both users use to encrypt their emails once more. So with the Goldbug, the user needs a kind of password (e.g. string based on AES) to open the e-mail of a friend or to be able to chat with him or read the message.

GoldBug (Software)

The GoldBug Messenger and E-Mail-Client is a user interface, which offers for the kernel and the application Spot-On an alternative to the originally offered user interface of Spot-on, which contains many options. Hence,

the GoldBug Graphical User Interface (GUI) is an own software compilation with the difference, that it provides a simplified interface. The name GoldBug for this software derives from a historical situation: The Gold Bug is a short story by Edgar Allan Poe, who made cryptograms popular: The plot is about William LeGrand, who recently encountered a gold-colored ladybug. His buddy, Jupiter, now expects LeGrand to evolve in his quest for insight, wealth, and wisdom after being in contact with the Golden Bug - and thus goes on to another friend of LeGrand, a narrator not further mentioned by name, who thinks it would be a good idea to visit his old friend again. After LeGrand then encountered a secret message and was able to decrypt it successfully, the three start an adventure as a team.



Figure 36: Logo/Headline „Instant Definition of Decentralized Crypto“ [PD]

Goppa Code

The binary Goppa code is an error-correcting code that belongs to the class of general Goppa codes originally described by Valerii Denisovich Goppa, but the binary

structure gives it several mathematical advantages over non-binary variants, also providing a better fit for common usage in computers and telecommunication. Binary Goppa codes have interesting properties suitable for cryptography in McEliece-like cryptosystems and similar setups.

Graph-Theory

In mathematics, and more specifically in graph theory, a graph is a representation of a set of objects where some pairs of objects are connected by links. The interconnected objects are represented by mathematical abstractions called vertices (also called nodes or points), and the links that connect some pairs of vertices are called edges (also called arcs or lines). Typically, a graph is depicted in diagrammatic form as a set of dots for the vertices, joined by lines or curves for the edges. Graphs are one of the objects of study in discrete mathematics. Common examples are a lattice graph or a Rook's graph.

Lattice graph: A lattice graph, mesh graph, or grid graph, is a graph whose drawing, embedded in some Euclidean space R^n , forms a regular tiling. This implies that the group of bijective transformations that send the graph to itself is a lattice in the group-theoretical sense. Typically, no clear distinction is made between such a graph in the more abstract sense of graph theory, and its drawing in space (often the plane or 3D space). This type of graph may more shortly be called just a lattice, mesh, or grid. Moreover, these terms are also commonly used for a finite section of the infinite graph, as in "an 8×8 square grid".

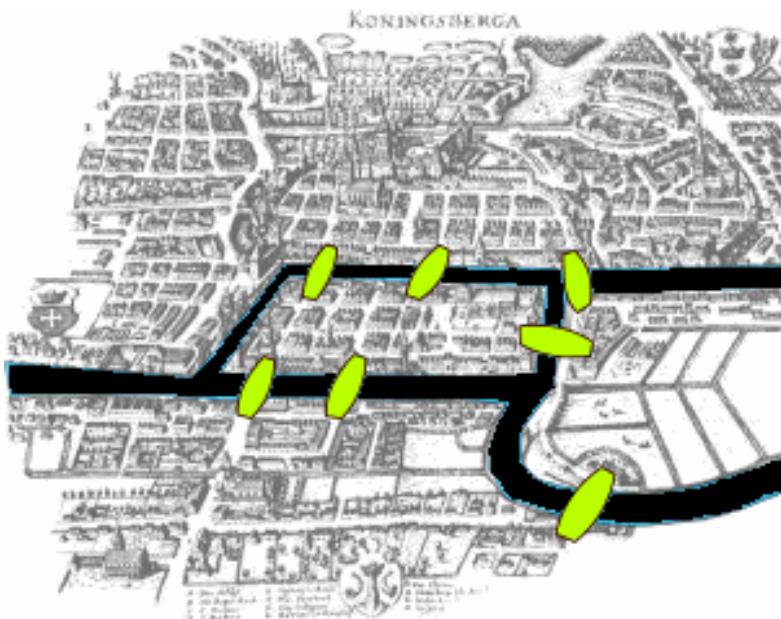


Figure 37: The Königsberg Bridge problem [PD]

The Seven Bridges of Königsberg is a historically notable problem in mathematics. Its negative resolution by Leonhard Euler in 1736 laid the foundations of graph theory and prefigured the idea of topology. The city of Königsberg in Prussia (now Kaliningrad, Russia) was set on both sides of the Pregel River, and included two large islands - Kneiphof and Lomse - which were connected to each other, or to the two mainland portions of the city, by seven bridges. The problem was to devise a walk through the city that would cross each of those bridges once and only once. By way of specifying the logical task unambiguously, solutions involving either reaching an island or mainland bank other than via one of the bridges, or accessing any bridge without crossing to its other end are explicitly unacceptable. Euler proved that the problem has no solution. The difficulty he faced was the development of a suitable technique of analysis, and of subsequent tests that established this assertion with mathematical rigor.

Rook's graph: A rook's graph is a graph that represents all legal moves of the rook chess piece on a chessboard. Each vertex of a rook's graph represents a square on a chessboard, and each edge represents a legal move from one square to another. Rook's graphs are highly symmetric.

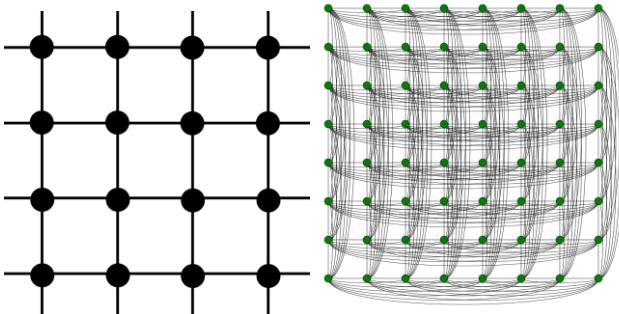


Figure 38: Lattice Square grid graph & 8x8 rook's graph: graph of possible moves for a standard chess rook [PD]

Group Chat

The term group chat, or group chat room, is primarily used to describe any form of synchronous conferencing, occasionally even asynchronous conferencing. The term can thus mean any technology ranging from real-time online chat and online interaction with strangers (e.g., online rooms) to fully immersive graphical social environments. The primary use of a group chat room is to share information via text with a group of other users. Generally speaking, the ability to converse with multiple people in the same conversation differentiates group chat rooms from instant messaging programs, which are more

typically designed for one-to-one communication - though two users also can define a group for private conversations.

GUI - Graphical User Interface

In computer science, a graphical user interface or GUI is a type of interface that allows users to interact with electronic devices through graphical icons and visual indicators such as secondary notation, as opposed to text-based interfaces, typed command labels or text navigation.

Half Echo

The open source Encryption Suite Spot-On provides two modes of operation for the there generally deployed Echo Protocol: Full Echo and Half Echo. The Full Echo permits absolute data flow. The Half Echo defines an agreement between two endpoints. Within this agreement, information from other endpoints is prohibited from traveling along the private channel. If one uses the modus "Half Echo", then the own message is not shared with other, third participants (Model: A -> B -> C). Only direct connections are used (Model A -> B). It requires only one direct connection to one friend. With the modus "Full Echo" the message is forwarded from friend to friend and so on to all connected neighbors, until the recipient could decrypt the envelope and read the message.

Hash Function

A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes. A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. These one-way hash functions have been called “the workhorses of modern cryptography”. The input data is often called the message, and the hash value is often called the message digest or simply the digest.

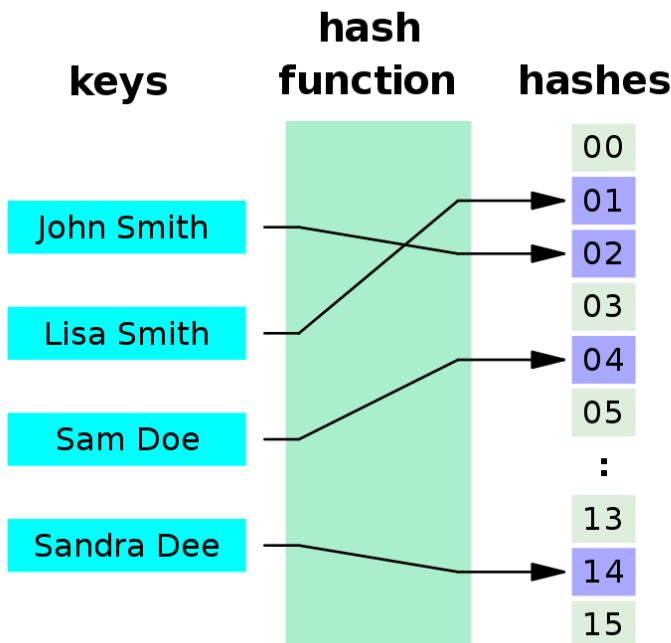


Figure 39: A perfect hash function for the four names shown [PD]

HMAC - Keyed-Hash Message Authentication Code

HMAC (sometimes expanded as either keyed-hash message authentication code or hash-based message authentication code) is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. It may be used to simultaneously verify both the data integrity and the authentication of a message, as with any MAC. Any cryptographic hash function, such as SHA-256 or SHA-3, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-X, where X is the hash function used (e.g. HMAC-SHA256 or HMAC-SHA3). The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and the size and quality of the key. HMAC uses two passes of hash computation. The secret key is first used to derive two keys – inner and outer. The first pass of the algorithm produces an internal hash derived from the message and the inner key. The second pass produces the final HMAC code derived from the inner hash result and the outer key. Thus, the algorithm provides better immunity against length extension attacks. An iterative hash function breaks up a message into blocks of a fixed size and iterates over them with a compression function. For example, SHA-256 operates on 512-bit blocks. The size of the output of HMAC is the same as that of the underlying hash function (e.g., 256 and 1600 bits in the case of SHA-256 and SHA-3, respectively), although it can be truncated if desired. HMAC does not encrypt the message. Instead, the message (encrypted or not) must be sent alongside the HMAC hash.

Parties with the secret key will hash the message again themselves, and if it is authentic, the received and computed hashes will match. The definition and analysis of the HMAC construction was first published in 1996 in a paper by Mihir Bellare, et al. and they also wrote RFC 2104.

Homomorphic Encryption

Homomorphic encryption is a form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. In algebra, a homomorphism is a structure-preserving map between two algebraic structures of the same type (such as two groups, two rings, or two vector spaces). The word homomorphism comes from the ancient Greek language: ὁμός (homos) meaning "same" and μορφή (morphe) meaning "form" or "shape". However, the word was apparently introduced to mathematics due to a (mis)translation of German “ähnlich” meaning "similar" to ὁμός meaning "same". Homomorphic encryption can be used for privacy-preserving outsourced storage and computation. This allows data to be encrypted and outsourced to commercial cloud environments for processing, all while encrypted. In highly regulated industries, such as health care, homomorphic encryption can be used to enable new services by removing privacy barriers inhibiting data sharing. For example, predictive analytics in health care can be hard to apply due to medical data privacy concerns, but if the predictive analytics service provider can

operate on encrypted data instead, these privacy concerns are diminished.

Homomorphic Secret Sharing

Homomorphic secret sharing is a type of secret sharing algorithm in which the secret is encrypted via homomorphic encryption. A homomorphism is a transformation from one algebraic structure into another of the same type so that the structure is preserved. Importantly, this means that for every kind of manipulation of the original data, there is a corresponding manipulation of the transformed data.

HTTPS

HTTPS (also called HTTP over TLS, HTTP over SSL, and HTTP Secure) is a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.

Human Rights

Human rights are the basic rights and freedoms to which all humans are entitled. Examples of rights and freedoms which are often thought of as human rights include civil

and political rights, such as the right to life, liberty, and property, freedom of expression, pursuit of happiness and equality before the law; and social, cultural and economic rights, including the right to participate in science and culture, the right to work, and the right to education and the right of privacy. All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood. - Article 1 of the United Nations Universal Declaration of Human Rights (UDHR). Civil and political rights are a class of rights that protect individuals' freedom from infringement by governments, social organizations, and private individuals. They ensure one's entitlement to participate in the civil and political life of the society and state without discrimination or repression. Civil rights include the ensuring of peoples' physical and mental integrity, life, and safety; protection from discrimination on grounds such as race, gender, sexual orientation, national origin, color, age, political affiliation, ethnicity, religion, and disability; and individual rights such as privacy and the freedom of thought, speech, religion, press, assembly, and movement. Political rights include natural justice (procedural fairness) in law, such as the rights of the accused, including the right to a fair trial; due process; the right to seek redress or a legal remedy; and rights of participation in civil society and politics such as freedom of association, the right to assemble, the right to petition, the right of self-defense, and the right to vote. Civil and political rights form the original and main part of international human rights. They comprise the first portion of the 1948 Universal Declaration of Human Rights (with

economic, social, and cultural rights comprising the second portion). The theory of three generations of human rights considers this group of rights to be "first-generation rights". Human rights applied to encryption is an important concept for freedom of expression as encryption is a technical resource of implementation of basic human rights. With the evolution of the digital age, application of freedom of speech becomes more controversial as new means of communication and restrictions arise including government control or commercial methods putting personal information to danger. From a human rights perspective, there is a growing awareness that encryption is an important piece of the puzzle for realizing a free, open and trustworthy Internet.



Figure 40: Eleanor Roosevelt and United Nations Universal Declaration of Human Rights in Spanish text [PD]

Hybrid Encryption

See also Multi-Encryption. Hybrid Encryption points especially out that symmetric and asymmetric encryption has been applied either in one application or to a plaintext or basically both or at least these two methods are mixed. E.g. a hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. Public-key cryptosystems are convenient in that they do not require the sender and receiver to share a common secret in order to communicate securely (among other useful properties). However, they often rely on complicated mathematical computations and are thus generally much more inefficient than comparable symmetric-key cryptosystems. In many applications, the high cost of encrypting long messages in a public-key cryptosystem can be prohibitive. This is addressed by hybrid systems by using a combination of both. A hybrid cryptosystem can be constructed e.g. using any two separate cryptosystems: 1. a key encapsulation scheme, which is a public-key cryptosystem, and 2. a data encapsulation scheme, which is a symmetric-key cryptosystem. The hybrid cryptosystem is itself a public-key system, whose public and private keys are the same as in the key encapsulation scheme. Note that for very long messages the bulk of the work in encryption/decryption is done by the more efficient symmetric-key scheme, while the inefficient public-key scheme is used only to encrypt/decrypt a short key value. All practical implementations of public key cryptography today employ the use of a hybrid system. Also, the use of more than one algorithm to encrypt ciphertext to ciphertext can be

regarded as a hybrid cryptosystem using e.g. the NTRU and then McEliece algorithm.

Identification

For data storage, identification is the capability to find, retrieve, report, change, or delete specific data without ambiguity. This applies especially to information stored in databases. In database normalisation, the process of organizing the fields and tables of a relational database to minimize redundancy and dependency, is the central, defining function of the discipline.

IMAP - Internet Message Access Protocol

In computing, the Internet Message Access Protocol (IMAP) is an Internet standard protocol used by e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection. IMAP is defined by RFC 3501. IMAP was designed with the goal of permitting complete management of an email box by multiple email clients, Therefore, clients generally leave messages on the server.

Impersonator

Impersonator is a function, which sends from the Spot-On encryption client a message from time to time into the Internet, which contains only random characters. With this method it is made more difficult for attackers to conduct time analysis of communications. Also, real cipher

text messages should be harder to recognize and harder to differ from such messages with random characters.

Information Security

Information security, sometimes shortened to InfoSec, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The information or data may take any form, e.g. electronic or physical. Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity. This is largely achieved through a multi-step risk management process that identifies assets, threat sources, vulnerabilities, potential impacts, and possible controls, followed by assessment of the effectiveness of the risk management plan. To standardize this discipline, academics and professionals collaborate and seek to set basic guidance, policies, and industry standards on password, antivirus software, firewall, encryption software, legal liability and user/administrator training standards. This standardization may be further driven by a wide variety of laws and regulations that affect how data is accessed, processed, stored, and transferred. However, the implementation of any standards and guidance within an entity may have limited effect if a culture of continual improvement isn't adopted.

Information-theoretic Security

Information-theoretic security is a cryptosystem whose security derives purely from information theory; the system cannot be broken even if the adversary has unlimited computing power. The cryptosystem is considered cryptanalytically unbreakable if the adversary does not have enough information to break the encryption. An encryption protocol with information-theoretic security does not depend for its effectiveness on unproven assumptions about computational hardness. Such a protocol is not vulnerable to future developments in computer power such as quantum computing. An example of an information-theoretically secure cryptosystem is the one-time pad. The concept of information-theoretically secure communication was introduced in 1949 by American mathematician Claude Shannon, the inventor of information theory, who used it to prove that the one-time pad system was secure. Information-theoretically secure cryptosystems have been used for the most sensitive governmental communications, such as diplomatic cables and high-level military communications, because of the great efforts enemy governments expend toward breaking them. Information security refers to preservation of confidentiality, integrity and availability of information.

Information Theory

Information theory studies the quantification, storage, and communication of information. It was originally proposed by Claude Shannon in 1948 to find fundamental limits on

signal processing and communication operations such as data compression, in a landmark paper entitled "A Mathematical Theory of Communication". Applications of fundamental topics of information theory include lossless data compression (e.g. ZIP files), lossy data compression (e.g. MP3s and JPEGs), and channel coding (e.g. for DSL). Its impact has been crucial to the success of the Voyager missions to deep space, the invention of the compact disc, the feasibility of mobile phones, the development of the Internet, the study of linguistics and of human perception, the understanding of black holes, and numerous other fields. A key measure in information theory is "entropy". Entropy quantifies the amount of uncertainty involved in the value of a random variable or the outcome of a random process. For example, identifying the outcome of a fair coin flip (with two equally likely outcomes) provides less information (lower entropy) than specifying the outcome from a roll of a die (with six equally likely outcomes). Some other important measures in information theory are mutual information, channel capacity, error exponents, and relative entropy. The field is at the intersection of mathematics, statistics, computer science, physics, neurobiology, information engineering, and electrical engineering. The theory has also found applications in other areas, including statistical inference, natural language processing, cryptography and many other.

Not to be confused with Information science: Information science is a field primarily concerned with the analysis, collection, classification, manipulation, storage, retrieval, movement, dissemination, and protection of information. Practitioners within and outside the field study application

and usage of knowledge in organizations along with the interaction between people, organizations, and any existing information systems with the aim of creating, replacing, improving, or understanding information systems.

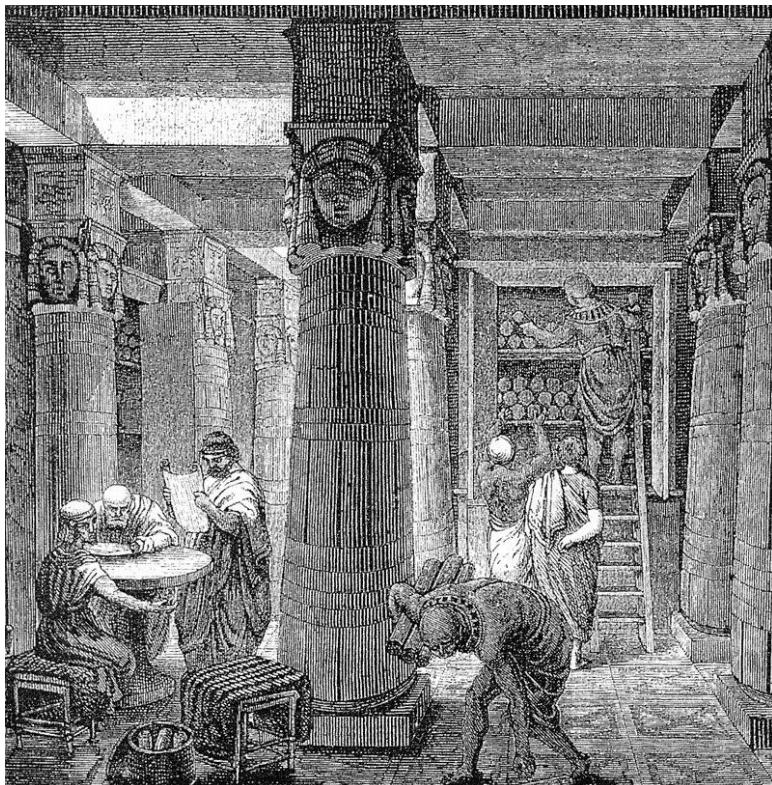


Figure 41: The Library of Alexandria [PD]

An early form of information storage and retrieval.

Innovation

Innovation in its modern meaning is a "new idea, creative thoughts, new imaginations in form of device or method". Innovation is often also viewed as the application of better solutions that meet new requirements, unarticulated needs, or existing market needs. Such innovation takes place through the provision of more-effective products, processes, services, technologies, or business models that are made available to markets, governments and society.

The POPTASTIC Protocol

Chat over E-Mail-Server Innovators & Early Adopters

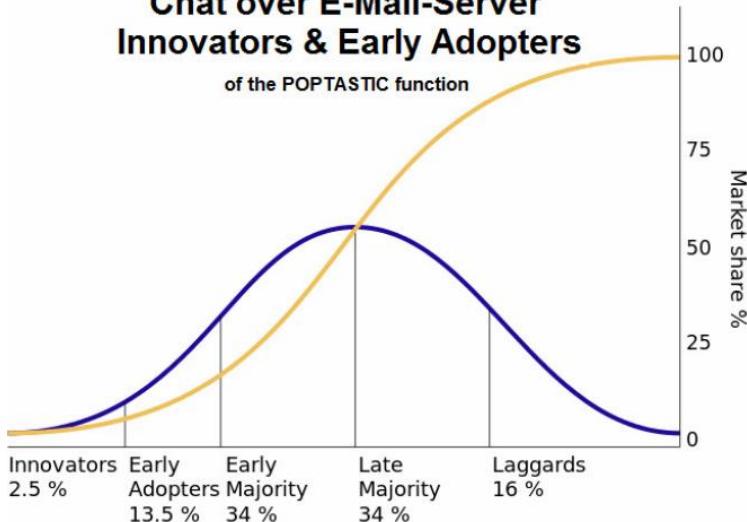


Figure 42: Early Adopters follow the Innovators for encrypted chat over e-mail servers [PD]

Rogers illustrates in his book "Diffusion of Innovations" (1962, 2003) the processes how innovation first by a group of the so called "innovators" and then by a group of "early adopters" is tested.

An innovation is something original and more effective and, as a consequence, new, that "breaks into" the market or society. Innovation is related to, but not the same as, invention, as innovation is more apt to involve the practical implementation of an invention (i.e. new/improved ability) to make a meaningful impact in the market or society, and not all innovations require an invention. As an example for innovation the POPTASTIC protocol with encrypted chat over e-mail-server can be regarded within cryptography and (chat) messaging.

Instant Messaging

Instant messaging (IM) technology is a type of online chat that offers real-time text transmission over the Internet. A LAN messenger operates in a similar way over a local area network. Short messages are typically transmitted between two parties, when each user chooses to complete a thought and select "send". Depending on the IM protocol, the technical architecture can be peer-to-peer (direct point-to-point transmission) or client-server (an Instant message service center retransmits messages from the sender to the communication device). By 2010, instant messaging over the Web was already in sharp decline, in favor of messaging features on social networks. The most popular IM platforms, such as AIM, closed in 2017, and Windows Live Messenger was merged into Skype. Today, most instant messaging takes place on messaging apps which by 2014 had more users than social networks. Major IM services are controlled by their corresponding companies. They usually follow the client-server model when all clients have to first

connect to the central server. This requires users to trust this server because messages can generally be accessed by the company. Companies can be compelled to reveal their user's communication. Companies can also suspend user accounts for any reason. There is the class of instant messengers that uses the serverless model, which doesn't require servers, and the IM network consists only of clients. There are several (mobile and) serverless messengers: Bitmessage, Ricochet, Ring, RetroShare, Tox. Serverless messengers are generally more secure because they involve fewer parties. Instant Messaging offers today Cryptographic Calling with end-to-end encryption or even Fiasco Forwarding and respective Fiasco Keys.

Institution

An Institution in Cryptography is an e-mail postbox to save messages for offline participants within a peer-to-peer network (e.g. deployed within clients for an Echo Network). The Institution is based on cryptographic credentials, so that in one node subscribed participant can deposit, save and retrieve messages with their public encryption key. The advantage despite other methods (e.g. storing the data within a common friend) is that the providing node of an Institution need not to give out the own public encryption key. The method, process and protocol for Institutions represent a kind of IMAP-Postbox within p2p e-mail. P2P e-mail might be - in a decentralized computing architecture - regarded as a potential successor for traditional client-server e-mail.

Integer Factorization

In number theory, integer factorization is the decomposition of a composite number into a product of smaller integers. If these integers are further restricted to prime numbers, the process is called prime factorization. When the numbers are sufficiently large, no efficient, non-quantum integer factorization algorithm is known. An effort by several researchers, concluded in 2009, to factor a 232-digit number (RSA-768) utilizing hundreds of machines took two years and the researchers estimated that a 1024-bit RSA modulus would take about a thousand times as long. However, it has not been proven that no efficient algorithm exists. The presumed difficulty of this problem is at the heart of widely used algorithms in cryptography such as RSA. Many areas of mathematics and computer science have been brought to bear on the problem, including elliptic curves, algebraic number theory, and quantum computing. Not all numbers of a given length are equally hard to factor. The hardest instances of these problems (for currently known techniques) are semiprimes, the product of two prime numbers. When they are both large, for instance more than two thousand bits long, randomly chosen, and about the same size (but not too close), even the fastest prime factorization algorithms on the fastest computers can take enough time to make the search impractical; that is, as the number of digits of the primes being factored increases, the number of operations required to perform the factorization on any computer increases drastically. Many cryptographic protocols are based on the difficulty of factoring large composite integers or a related problem. An algorithm that efficiently factors

an arbitrary integer would render RSA-based public-key cryptography insecure.

Integrity

Integrity is a property of accuracy and completeness. Data integrity is the maintenance of, and the assurance of the accuracy and consistency of, data over its entire life-cycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data. The term is broad in scope and may have widely different meanings depending on the specific context – even under the same general umbrella of computing. It is at times used as a proxy term for data quality, while data validation is a pre-requisite for data integrity. Data integrity is the opposite of data corruption. And: In telecommunications, the term system integrity has the following meanings: That condition of a system wherein its mandated operational and technical parameters are within the prescribed limits. The quality of an automated information system (AIS) when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. The state that exists when there is complete assurance that under all conditions an IT system is based on the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanisms, and data integrity.

Internet

The Internet is the publicly available worldwide system of interconnected computer networks that transmit data by packet switching over the Internet Protocol (IP). It is made up of thousands of other, smaller business, academic, and government networks. The terms Internet and World Wide Web are often used in every-day speech without much distinction. However, the Internet and the World Wide Web are not one and the same. The Internet is a global data communications system. It is a hardware and software infrastructure that provides connectivity between computers. Simply, the "Internet is a network of networks", where two or more than two computers are connected through a wired or wireless network for sending and receiving data - such as text, video, songs, etc. In contrast, the Web is one of the services communicated via the Internet. The Web is a collection of interconnected documents and other resources, linked by hyperlinks and URLs. Other services using the internet include electronic mail, File Transfer Protocol, Telnet, online chat, Voice over Internet Protocol, Instant messaging, Fax, and Usenet.

Internet Security

Internet security is a branch of computer security specifically related to not only the Internet, often involving browser security and the World Wide Web, but also network security as it applies to other applications or operating systems as a whole. Its objective is to establish rules and measures to use against attacks over the Internet.

The Internet represents an insecure channel for exchanging information, which leads to a high risk of intrusion or fraud, such as phishing, online viruses, trojans, worms and more. Many methods are used to protect the transfer of data, including encryption and from-the-ground-up engineering. The current focus is on prevention as much as on real time protection against well-known and new threats.

IPFS - Instant Perfect Forward Secrecy

IPFS is the abbreviation of Instant Perfect Forward Secrecy. While Perfect Forward Secrecy, often also called only Forward Secrecy, describes within many applications and as well from a conceptional approach the transmission of ephemeral - this means temporary - keys, it is implicit connected, that this is proceeded one time per online session. With the open source Encryption Suite Spot-On and the underlying architecture of the Spot-On Kernel a new paradigm has been implemented: Forward Secrecy or Perfect Forward Secrecy, has developed further to Instant Perfect Forward Secrecy (IPFS). While Forward Secrecy means to be able to neglect to have used a certain key in the past if one further key is compromised, this concept addresses to end-to-end encryption. With Instant Perfect Forward Secrecy the Cryptographic Calling comes into the frame: A user is able to renew the end-to-end encrypting credentials like in a phone call: Instantly and several times within a session the user should be able to renew temporary keys for end-to-end encryption. An even further development of this concept has been taken place by the development of Fiasco Forwarding, which sends a full

bundle of keys within one session or with a(n automated) call action for future sessions. The end-to-end-encryption with temporary keys can be changed at any time, this means also per any second. This describes the term of Instant Perfect Forward Secrecy (IPFS). Via a so-called “Call” the end-to-end-encryption can be renewed: Instantly. Also, the term of a “call” for the transmission of a to-be-created or to-be-renewed end-to-end-encryption has been introduced by the application Spot-On (see early documentation) into Cryptography.

IRC – Internet Relay Chat

Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in the form of text. The chat process works on a client/server networking model. IRC clients are computer programs that users can install on their system or web-based applications running either locally in the browser or on 3rd party server. These clients communicate with chat servers to transfer messages to other clients. IRC is mainly designed for group communication in discussion forums, called channels, but also allows one-on-one communication via private messages as well as chat and data transfer, including file sharing. The encrypted group chat in IRC style of an Echo network is called Buzz or e*IRC chat.

Isomorphism

In mathematics, an isomorphism (from the Ancient Greek: ἴσος isos "equal", and μορφή morphe "form" or "shape") is

a homomorphism or morphism (a structure-preserving map from one mathematical structure to another one of the same type: i.e. a mathematical mapping) that can be reversed by an inverse morphism. Two mathematical objects are isomorphic if an isomorphism exists between them. An automorphism is an isomorphism whose source and target coincide. The interest of isomorphisms lies in the fact that two isomorphic objects cannot be distinguished by using only the properties used to define morphisms; thus isomorphic objects may be considered the same as long as one considers only these properties and their consequences.

Iterated Function

In mathematics, an iterated function is a function $X \rightarrow X$ (that is, a function from some set X to itself) which is obtained by composing another function $f: X \rightarrow X$ with itself a certain number of times. The process of repeatedly applying the same function is called iteration. Iterated functions are objects of study in computer science, fractals, dynamical systems, mathematics and renormalization group physics.

Java

Java is a general-purpose computer-programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere" (WORA), meaning

that compiled Java code can run on all platforms that support Java without the need for recompilation.

Juggerknots / Juggerknot Keys

Juggerknots respective Juggerknot Keys are keys, which are derived by the Juggernaut Protocol also known as Juggling PAKE (J-PAKE) protocol. That means a JuggerKnot is a stream of private data: The stream is generated from the results of a successful Juggernaut execution. Here similar to the SMP Socialist Millionaire Protocol two users enter the same password and over a zero-knowledge-proof process the authentication of both users and the fitting password on both sites is verified without transferring the common secret over the internet. While in the application Spot-On in the Secret Streams function the SMP protocol is used, in the Smoke Crypto Messenger the Juggernaut JPAKE protocol with a similar process is implemented. Secret Stream Keys are derived from the SMP protocol and Juggerknot Keys are derived from the Juggling J-Pake protocol, known as Juggernaut protocol. Both variants are mathematically breathtaking, as the keys for encryption are not transferred over the internet. The Key transfer problem is solved with Secret Streams and Juggerknot keys. Kerckhoffs' Principle – to keep the key secret – even for asymmetric keys, is fostered with these two protocols of Juggerknots (keys) (and keys derived within the Secret Streams protocol process). While the new direction in the 1970 by Diffie/Hellman was, to invent a method to share a – public key – in a semi secure channel, the new direction of the programmers of the applications of Spot-On (for

Secret Streams) and Smoke Messenger (for Juggerknot Keys) is that the keys need not to be transferred over any channel any more! A new cesura by incorporating a mathematically breathtaking zero-knowledge-proof process.

Juggernaut PAKE Protocol

The Password Authenticated Key Exchange by Juggling (or J-PAKE) is a password-authenticated key agreement protocol, proposed by Feng Hao and Peter Ryan. This protocol allows two parties to establish private and authenticated communication solely based on their shared (low-entropy) password without requiring a Public Key Infrastructure. It provides mutual authentication to the key exchange, a feature that is lacking in the Diffie-Hellman key exchange protocol. Two parties, Alice and Bob, agree on a group G with generator g of prime order q in which the discrete log problem is hard. In general, J-PAKE can use any prime order group that is suitable for public key cryptography, including Elliptic curve cryptography. Let's be their shared (low-entropy) secret, which can be a password or a hash of a password. The protocol executes in two rounds. The earliest record of juggling is suggested in a panel from the 15th (1994 to 1781 B.C.) Beni Hasan tomb of an unknown Egyptian prince, showing female dancers and acrobats throwing balls. Mathematics has been used to understand juggling and juggling has been used to test mathematics. The Messenger Smoke implements the Password Authenticated Key Exchange by Juggling protocol (Juggernaut PAKE Protocol). The data for the zero-

knowledge proof is exchanged within a messaging session and several rounds.

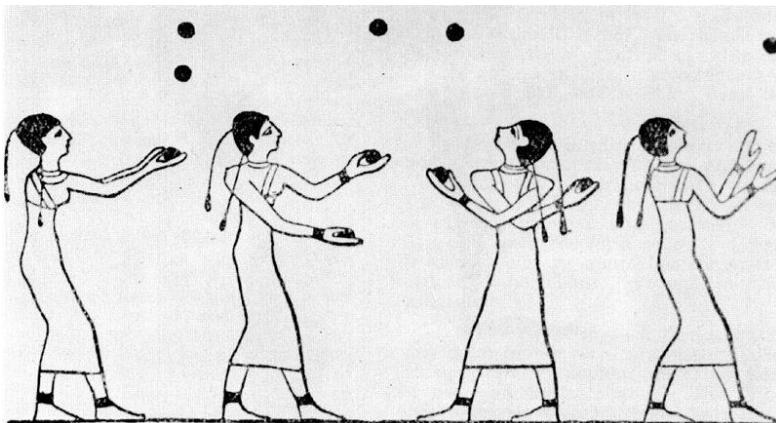


Figure 43: Jugglers within the Karyssa I area, Egypt: Testing the truth [PD]

This ancient wall painting appears to depict jugglers. It was found in the 15th tomb of the Karyssa I area, Egypt. According to Dr. Bianchi, associate curator of the Brooklyn Museum "In tomb 15, the prince is looking on to things he enjoyed in life that he wishes to take to the next world. The fact that jugglers are represented in a tomb suggests religious significance." ... "round things were used to represent large solar objects, birth, and death."

The name of the protocol may derive from a comic character: Juggernaut (Cain Marko) is a fictional character appearing in American comic books published by Marvel Comics. The character, who first appeared in X-Men #12 (July 1965), was created by writer Stan Lee and artist/co-writer Jack Kirby. When Cain Marko finds the Gem of the mystical entity Cyttorak, he is empowered with magical energies and transformed into an immortal avatar for the entity in question. As the Juggernaut, Marko possesses

superhuman strength, being capable of shattering mountains, lifting and using buildings as weapons, and extreme durability. Juggernaut is able to generate a mystical force field that grants him additional invulnerability to any physical attack when it is at its maximum. The character is vulnerable to mental attacks, a weakness that has been exploited via the removal of his helmet, which normally protects him from such. The Juggernaut has circumvented this weakness on occasion by wearing a metal skullcap inside his main helmet. If Juggernaut loses his helmet, he can magically recreate it from available raw materials (as long as he possesses the full power of the gem). As an analogy to the encryption protocol: Both communication partners need only their minds, not a key transfer.

KDF - Key Derivation Function

A key derivation function (KDF) derives one or more secret keys from a secret value such as a master key, a password, or a passphrase using a pseudorandom function. KDFs can be used to stretch keys into longer keys or to obtain keys of a required format, such as converting a group element that is the result of a Diffie-Hellman key exchange into a symmetric key for use with AES. Keyed cryptographic hash functions are popular examples of pseudorandom functions used for key derivation. Key derivation functions are also used in applications to derive keys from secret passwords or passphrases, which typically do not have the desired properties to be used directly as cryptographic keys. In such applications, it is generally recommended that the key

derivation function be made deliberately slow so as to frustrate brute-force attack or dictionary attack on the password or passphrase input value. Such use may be expressed as $DK = KDF(key, salt, iterations)$, where DK is the derived key, KDF is the key derivation function, key is the original key or password, salt is a random number which acts as cryptographic salt, and iterations refers to the number of iterations of a sub-function. The derived key is used instead of the original key or password as the key to the system. The values of the salt and the number of iterations (if it is not fixed) are stored with the hashed password or sent as plaintext with an encrypted message. The difficulty of a brute force attack increases with the number of iterations. A practical limit on the iteration count is the unwillingness of users to tolerate a perceptible delay in logging into a computer or seeing a decrypted message. The use of salt prevents the attackers from precomputing a dictionary of derived keys. An alternative approach, called key strengthening, extends the key with a random salt, but then (unlike in key stretching) securely deletes the salt. This forces both, the attacker and legitimate users, to perform a brute-force search for the salt value.

Kerberos

Kerberos is a computer network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Kerberos builds on symmetric key cryptography and requires a trusted third

party, and optionally may use public-key cryptography during certain phases of authentication. The protocol was named after the character Kerberos (or Cerberus) from Greek mythology, the ferocious three-headed guard dog of Hades. Its designers aimed it primarily at a client–server model and it provides mutual authentication — both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

Kerckhoffs' Principle

Kerckhoffs' principle was stated by Netherlands born cryptographer Auguste Kerckhoffs in the 19th century: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge. Kerckhoffs' principle was reformulated (or possibly independently formulated) by American mathematician Claude Shannon as "the enemy knows the system", i.e., "one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them". In that form, it is called Shannon's maxim. Kerckhoffs' principle (Shannon's maxim) is widely embraced by cryptographers.

Kernel

In computing, the kernel is a computer program that manages input/output requests from software and translates them into data processing instructions for the central processing unit and other electronic components of

a computer. The kernel is a fundamental part of a modern computer's operating system or of applications.

Key

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms. Keys also specify transformations in other cryptographic algorithms, such as digital signature schemes and message authentication codes. In designing security systems, it is wise to assume that the details of the cryptographic algorithm are already available to the attacker. This is known as Kerckhoffs' principle — "only secrecy of the key provides security", or, reformulated as Shannon's maxim, "the enemy knows the system". The history of cryptography provides evidence that it can be difficult to keep the details of a widely used algorithm secret. A key is often easier to protect (it's typically a small piece of information) than an encryption algorithm, and easier to change if compromised. Thus, the security of an encryption system in most cases relies on some key being kept secret. Trying to keep keys secret is one of the most difficult problems in practical cryptography; see key management. An attacker who obtains the key (by, for example, theft, extortion, dumpster diving, assault, torture, or social engineering) can recover the original message from the encrypted data, and issue signatures.

Keyboard

In computing, a computer keyboard is a typewriter-style device which uses an arrangement of buttons or keys to act as mechanical levers or electronic switches. Keyboard keys (buttons) typically have characters engraved or printed on them, and each press of a key typically corresponds to a single written symbol. Virtual keyboards in software with encryption prevent that key-loggers record the typing - as mouse clicks do not indicate, which symbol has been clicked.

Key Exchange / Establishment

Key management refers to management of cryptographic keys in a cryptosystem. A key can be in the hand of both users or in the hand of third party, managing a key exchange. Ideally a key is not in the hand of a third party, regardless if it is a symmetric or asymmetric key. Key management includes dealing with the generation, exchange, storage, use, crypto-shredding (destruction) and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols. Key management concerns keys at the user level, either between users or systems. This is in contrast to key scheduling, which typically refers to the internal handling of keys within the operation of a cipher. Successful key management is critical to the security of a cryptosystem. It is the more challenging side of cryptography in a sense that it involves aspects of social engineering such as system policy, user training, organizational and departmental

interactions, and coordination between all of these elements, in contrast to pure mathematical practices that can be automated. Hence, Key exchange (also key establishment) is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key. Prior to any secured communication, users must set up the details of the cryptography. In some instances, this may require exchanging identical keys (in the case of a symmetric key system). In others it may require possessing the other party's public key. While public keys can be openly exchanged (their corresponding private key is kept secret), symmetric keys must be exchanged over a secure communication channel. Formerly, exchange of such a key was extremely troublesome, and was greatly eased by access to secure channels such as a diplomatic bag. Clear text exchange of symmetric keys would enable any interceptor to immediately learn the key, and any encrypted data. The key exchange problem describes ways to exchange whatever keys or other information are needed for establishing a secure communication channel so that no one else can obtain a copy. Historically, before the

invention of public-key cryptography (asymmetrical cryptography), symmetric-key cryptography utilized a single key to encrypt and decrypt messages. For two parties to communicate confidentially, they must first exchange the secret key so that each party is able to encrypt messages before sending, and decrypt received ones. This process is known as the key exchange. The overarching problem with symmetrical cryptography, or single-key cryptography, is that it requires a secret key to be communicated through trusted couriers, diplomatic bags, or any other secure communication channel. If two parties cannot establish a secure initial key exchange, they won't be able to communicate securely without the risk of messages being intercepted and decrypted by a third party who acquired the key during the initial key exchange. Public-key cryptography uses a two-key system, consisting of the public and the private keys, where messages are encrypted with one key and decrypted with another. It depends on the selected cryptographic algorithm which key - public or private - is used for encrypting messages, and which for decrypting. For example, in RSA, the private key is used for decrypting messages, while in the Digital Signature Algorithm (DSA), the private key is used for encrypting them. The public key can be sent over non-secure channels or shared in public; the private key is only available to its owner. The advance of public key cryptography in the 1970s has made the exchange of keys less troublesome. Since the Diffie-Hellman key exchange protocol was published in 1975, it has become possible to exchange a key over an insecure communications channel, which has substantially reduced the risk of key disclosure during

distribution. It is possible, using something akin to a book code, to include key indicators as clear text attached to an encrypted message. Known as the Diffie-Hellman key exchange, the encryption key can be openly communicated as it poses no risk to the confidentiality of encrypted messages. One party exchanges the keys to another party where they can then encrypt messages using the key and send back the ciphertext. Only the decryption key - in this case, it's the private key - can decrypt that message. At no time during the Diffie-Hellman key exchange is any sensitive information at risk of compromise, as opposed to symmetrical key exchange. The encryption technique used by Richard Sorge's code clerk was of this type, referring to a page in a statistical manual, though it was in fact a code. The German Army Enigma symmetric encryption key was a mixed type early in its use; the key was a combination of secretly distributed key schedules and a user chosen session key component for each message. In more modern systems, such as OpenPGP compatible systems, a session key for a symmetric key algorithm is distributed encrypted by an asymmetric key algorithm. This approach avoids even the necessity for using a key exchange protocol like Diffie-Hellman key exchange. Another method of key exchange involves encapsulating one key within another. Typically, a master key is generated and exchanged using some secure method. This method is usually cumbersome or expensive (breaking a master key into multiple parts and sending each with a trusted courier for example) and not suitable for use on a larger scale. Once the master key has been securely exchanged, it can then be used to securely exchange subsequent keys with ease. This technique is usually

termed key wrap. A common technique uses block ciphers and cryptographic hash functions. A related method is to exchange a master key (sometimes termed a root key) and derive subsidiary keys as needed from that key and some other data (often referred to as diversification data). The most common use for this method is probably in smartcard-based cryptosystems, such as those found in banking cards. The bank or credit network embeds their secret key into the card's secure key storage during card production at a secured production facility. Then at the point of sale the card and card reader are both able to derive a common set of session keys based on the shared secret key and card-specific data (such as the card serial number). This method can also be used when keys must be related to each other (i.e., departmental keys are tied to divisional keys, and individual keys tied to departmental keys). However, tying keys to each other in this way increases the damage which may result from a security breach as attackers will learn something about more than one key. This reduces entropy, with regard to an attacker, for each key involved. Today keys are also broadcasted in secure EPKS channels (for symmetric and asymmetric keys) or via AutoCrypt (for asymmetric public keys). Most modern are key derivations which are not based on a key exchange, but rather a derivation from a SMP (Secret Streams) or JPAKE Process: Juggerknot keys. In this case keys are established via a zero-knowledge-proof process and are not transferred over the internet or any channel. Juggerknot Keys are implemented in the Crypto Messenger Smoke and Secret Stream Keys are implemented in the Spot-On Encryption Suite Software.

Key Size

Key size or key length is the number of bits in a key used by a cryptographic algorithm (such as a cipher). Key length defines the upper-bound on an algorithm's security (i.e., a logarithmic measure of the fastest known attack against an algorithm, relative to the key length), since the security of all algorithms can be violated by brute-force attacks. Ideally, key length would coincide with the lower-bound on an algorithm's security. Indeed, most symmetric-key algorithms are designed to have security equal to their key length. Nevertheless, as long as the relation between key length and security is sufficient for a particular application, then it doesn't matter if key length and security coincide. This is important for asymmetric-key algorithms, because no such algorithm is known to satisfy this property; elliptic curve cryptography comes the closest with an effective security of roughly half its key length. Keys are used to control the operation of a cipher so that only the correct key can convert encrypted text (ciphertext) to plaintext. Many ciphers are actually based on publicly known algorithms or are open source and so it is only the difficulty of obtaining the key that determines security of the system, provided that there is no analytic attack (i.e., a 'structural weakness' in the algorithms or protocols used), and assuming that the key is not otherwise available (such as via theft, extortion, or compromise of computer systems). The widely accepted notion that the security of the system should depend on the key alone has been explicitly formulated by Auguste Kerckhoffs (in the 1880s) and Claude Shannon (in the 1940s); the statements are known as Kerckhoffs' principle and Shannon's Maxim respectively.

A key should therefore be large enough that a brute-force attack (possible against any encryption algorithm) is infeasible – i.e., would take too long to execute. Shannon's work on information theory showed that to achieve so called perfect secrecy, the key length must be at least as large as the message and only used once (this algorithm is called the One-time pad). In light of this, and the practical difficulty of managing such long keys, modern cryptographic practice has discarded the notion of perfect secrecy as a requirement for encryption, and instead focuses on computational security, under which the computational requirements of breaking an encrypted text must be infeasible for an attacker.

Key Stretching

Key stretching techniques are used to make a possibly weak key, typically a password or passphrase, more secure against a brute-force attack by increasing the resources (time and possibly space) it takes to test each possible key. Passwords or passphrases created by humans are often short or predictable enough to allow password cracking, and key stretching is intended to make such attacks more difficult by complicating a basic step of trying a single password candidate. Because a key generation function must be deterministic so that the weak key always generates the same stretched key (called an enhanced key), the stretching of the key does not alter the entropy of the key-space, only complicates the method of computing the enhanced key. Attacks on unsalted key stretching functions exist called rainbow tables. Salting the key is the process of

appending a long, random string to the weak key. This is done so that precomputed hashes of either short keys or password lists cannot be used in authentication schemes that require the hash to be presented or to reverse hashes into their original pass-phrases which may be used to compromise users on other services using the same passphrase. Key stretching techniques generally work as follows. The initial key is fed into an algorithm that outputs an enhanced key. The enhanced key should be of sufficient size to make it infeasible to break by brute force (e.g. 128 bits). The overall algorithm used should be secure in the sense that there should be no known way of taking a shortcut that would make it possible to calculate the enhanced key with less processor work and memory used than by using the key stretching algorithm itself. The key stretching process leaves the attacker with two options: either try every possible combination of the enhanced key (infeasible if the enhanced key is long enough), or else try likely combinations of the initial key. In the latter approach, if the initial key is a password or a passphrase, then the attacker would first try every word in a dictionary or common password list and then try all character combinations for longer passwords. Key stretching does not prevent this approach, but the attacker has to spend much more resources (time and/or memory used) on each attempt, which may easily make this approach infeasible as well. If the attacker uses the same class of hardware as the user, each guess will take the similar amount of time to process as it took the user (for example, one second). Even if the attacker has much greater computing resources than the user, the key stretching will still slow the attacker down

while not seriously affecting the usability of the system for any legitimate user, since the user's computer only has to compute the stretching function once upon the user entering their password, whereas the attacker must compute it for every guess in the attack. There are several ways to perform key stretching. One way is to apply a cryptographic hash function or a block cipher repeatedly in a loop. E.g., in applications where the key is used for a cipher, the key schedule in the cipher may be modified so that it takes a specific length of time to perform. Another way is to use cryptographic hash functions that have large memory requirements – these can be effective in frustrating attacks by memory-bound adversaries. A related technique, salting, protects against attacks that take advantage of certain time–memory trade-offs (which often utilize some variation of rainbow tables) and is often used in conjunction with key stretching.

Keystroke Logging

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. A keylogger can be either software or hardware. While the programs themselves are legal, with many of them being designed to allow employers to oversee the use of their computers, keyloggers are most often used for the purpose of stealing passwords and other confidential information. Keylogging

can also be used to study human–computer interaction. Numerous keylogging methods exist: they range from hardware and software-based approaches to acoustic analysis.

KeySync

KeySync is a term deriving from the context of the term AutoCrypt, which are both a follow up of the idea of a REPLEO, respective a key exchange over the EPKS – Echo Public Key Sharing – Protocol. Here two participants share over a channel the public keys and integrate the received keys into the own nodes or instances.

Lattice-based Cryptography

Lattice-based cryptography is the generic term for constructions of cryptographic primitives that involve lattices, either in the construction itself or in the security proof. Lattice-based constructions are currently important candidates for post-quantum cryptography. Unlike more widely used and known public-key schemes such as the RSA, Diffie-Hellman or Elliptic-Curve cryptosystems, which are easily attacked by a quantum computer, some lattice-based constructions appear to be resistant to attack by both classical and quantum computers. Furthermore, many lattice-based constructions are known to be secure under the assumption that certain well-studied computational lattice problems cannot be solved efficiently. In 1996, Miklós Ajtai introduced the first lattice-based cryptographic construction whose security could be based on the

hardness of well-studied lattice problems. Fundamentally, Ajtai's result was a worst-case to average-case reduction. I.e., he showed that a certain average-case lattice problem (known as Short Integer Solutions (SIS)) is at least as hard to solve as a worst-case lattice problem. He then showed a cryptographic hash function whose security is equivalent to the computational hardness of SIS. In 1998, Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman introduced a lattice-based public-key encryption scheme, known as NTRU. The first lattice-based public-key encryption scheme whose security was proven under worst-case hardness assumptions was introduced by Oded Regev in 2005, together with the Learning with Errors problem (LWE). Since then, much follow-up work has focused on improving Regev's security proof and improving the efficiency of the original scheme. Much more work has been devoted to constructing additional cryptographic primitives based on LWE and related problems. For example, in 2009, Craig Gentry introduced the first fully homomorphic encryption scheme, which was based on a lattice problem. Lattice-based cryptographic constructions are the leading candidates for public-key post-quantum cryptography. Indeed, the main alternative forms of public-key cryptography are schemes based on the hardness of factoring and related problems and schemes based on the hardness of the discrete logarithm and related problems. Many lattice-based cryptographic schemes are known to be secure assuming the worst-case hardness of certain lattice problems.

Libcurl

cURL is a computer software project providing a library and command-line tool for transferring data using various protocols. The cURL project produces two products, libcurl and curl. It was first released in 1997. The name originally stood for “see URL”.

Libgcrypt

Libgcrypt is a cryptography library developed as a separated module of GnuPG. It can also be used independently of GnuPG, but depends on its error-reporting library Libgpg-error. Libgcrypt features its own multiple precision arithmetic implementation, with assembler implementations for a variety of processors, including Alpha, AMD64, HP PA-RISC, i386, i586, M68K, MIPS 3, PowerPC, and SPARC. It also features an entropy gathering utility, coming in different versions for Unix-like and Windows machines. As for GnuPG, multiple branches of Libgcrypt are maintained in parallel, currently the branch 1.8.

LibSpotOn

LibSpotOn is the library written in C++ for the Echo Protocol and kernel.

Listener

A listener is a software design pattern in which an object maintains a list of its dependents and notifies them automatically of any state changes, usually by calling one of their methods. It is mainly used to implement distributed event handling systems. It is often used for creating or opening a port on which the service or chat-server then is "listening" for incoming data connections.

Login

In computer security, logging in (or logging on or signing in or signing on) is the process by which an individual gains access to a computer system by identifying and authenticating themselves. The user credentials are typically some form of "username" and a matching "password", and these credentials themselves are sometimes referred to as a login, (or a logon or a sign-in or a sign-on).

MAC - Message Authentication Code

A message authentication code (often MAC) is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message. Integrity assurances detect accidental and intentional message changes, while authenticity assurances affirm the message's origin. A MAC algorithm, sometimes called a keyed (cryptographic) hash function (however, cryptographic hash function is only one of the possible

ways to generate MACs), accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

Magnet-URI

The Magnet-URI scheme defines the format of Magnet-links, a de facto standard for identifying files by their content, e.g. via cryptographic hash values rather than by their location. Within cryptography the Magnet-URI scheme has been developed further, so that the Magnet link holds different cryptographic values, such as cipher, hash, or hash key or channel key. The extension URN defines the usage of that Magnet link, e.g. to open a chat room or to define a usage for e-mail or e-mail post boxes, which are found p2p on a network.

Magnet-URI with cryptographical values

```
Magnet:?rn=Channel_Key  
    &xf=10000  
    &xs=Channel_Salt  
    &ct=aes256  
    &hk=Channel_Hash_Key  
    &ht=sha512  
    &xt=urn:buzz
```

Figure 44: Example of a Magnet-URI with cryptographic values (here for a group chat Buzz channel) [PD]

Several abbreviations refer to different cryptographic values, which can be embedded into such a Magnet URI link as a standard.

Abbreviation	Example	Description
rn	&rn=Channel_Key	Roomname
xf	&xf=10000	Exact Frequency
xs	&xs=Channel_Salt	Exact Salt
ct	&ct=aes256	Cipher Type
hk	&hk=Channel_Hash_Key	Hash Key
ht	&ht=sha512	Hash Type
xt=urn:buzz	&xt=urn:buzz	Magnet for IRC Chat
xt=urn:starbeam	&xt=urn:starbeam	Magnet for filetransfer
xt=urn:institution	&xt=urn:institution	Magnet for the virtual e-mail-Postbox

Figure 45: Cryptographic values for the Magnet-URI standard as they are used by some encryption applications (PD)

Malleability

Malleability is a property of some cryptographic algorithms. An encryption algorithm is "malleable" if it is possible to transform a ciphertext into another ciphertext which decrypts to a related plaintext. That is, given an encryption of a plaintext m , it is possible to generate another ciphertext which decrypts to $f(m)$, for a known function f , without necessarily knowing or learning m . Malleability is often an undesirable property in a general-purpose cryptosystem, since it allows an attacker to modify the contents of a message. For example, suppose that a bank uses a stream cipher to hide its financial information, and a user sends an encrypted message containing, say,

"TRANSFER \$0000100.00 TO ACCOUNT #199." If an attacker can modify the message on the wire, and can guess the format of the unencrypted message, the attacker could be able to change the amount of the transaction, or the recipient of the funds, e.g. "TRANSFER \$0100000.00 TO ACCOUNT #227". Malleability does not refer to the attacker's ability to read the encrypted message. Both before and after tampering, the attacker cannot read the encrypted message. On the other hand, some cryptosystems are malleable by design. In other words, in some circumstances it may be viewed as a feature that anyone can transform an encryption of m into a valid encryption of $f(m)$ (for some restricted class of functions f) without necessarily learning m . Such schemes are known as homomorphic encryption schemes.

Mass Surveillance

Mass surveillance is the intricate surveillance of an entire or a substantial fraction of a population in order to monitor that group of citizens. The surveillance is often carried out by local and federal governments or governmental organisations, such as organizations like the NSA and the FBI, but it may also be carried out by corporations (either on behalf of governments or at their own initiative). Depending on each nation's laws and judicial systems, the legality of and the permission required to engage in mass surveillance varies. It is the single most indicative distinguishing trait of totalitarian regimes. It is also often distinguished from targeted surveillance. Mass surveillance has often been cited as necessary to fight terrorism,

prevent crime and social unrest, protect national security, and control the population. Conversely, mass surveillance has equally often been criticized for violating privacy rights, limiting civil and political rights and freedoms, and being illegal under some legal or constitutional systems. Another criticism is that increasing mass surveillance could lead to the development of a surveillance state or an electronic police state where civil liberties are infringed, or political dissent is undermined. Such a state could be referred to as a totalitarian state. In 2013, the practice of mass surveillance by world governments was called into question after Edward Snowden's 2013 global surveillance disclosure. Reporting based on documents Snowden leaked to various media outlets triggered a debate about civil liberties and the right to privacy in the Digital Age. Mass surveillance is considered a global issue.

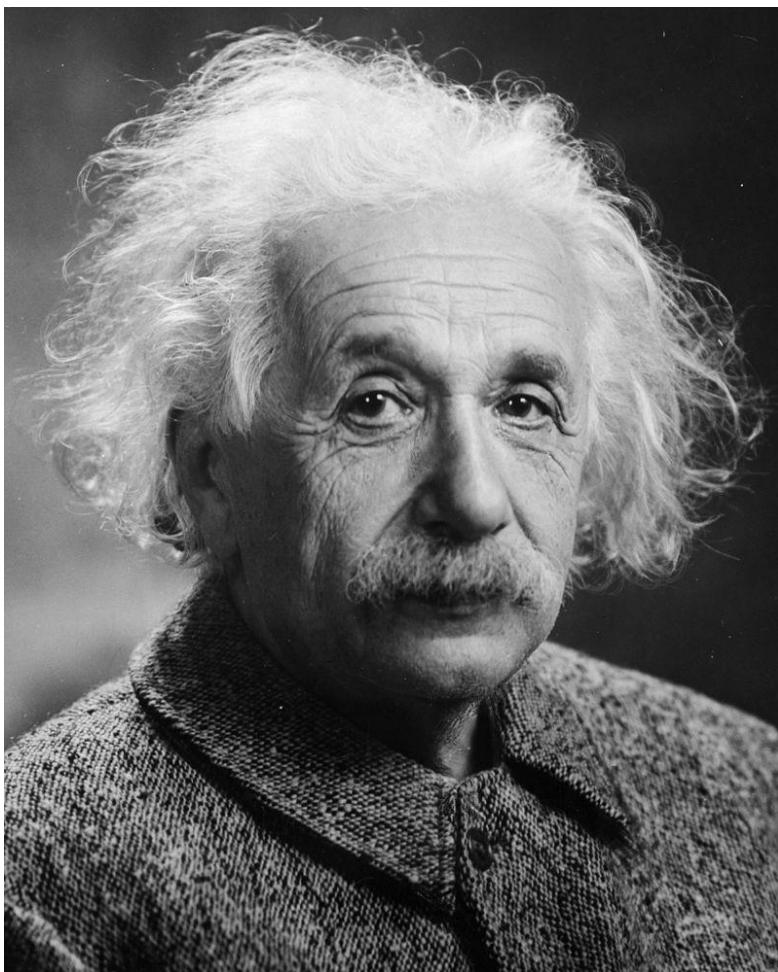


Figure 46: Albert Einstein was placed under surveillance due to his alleged ties to communism [PD]

Due to his alleged ties to communism, the German-born physicist Albert Einstein was placed under surveillance by the Federal Bureau of Investigation (FBI) shortly after he emigrated to America. The FBI monitored Einstein's mail, intercepted his telephone calls, and searched his trash.

Matrix

Matrix is an open standard and lightweight protocol for real-time communication. It is designed to allow users with accounts at one communications service provider to communicate with users of a different service provider via online chat, voice over IP, and videotelephony. That is, it aims to make real-time communication work seamlessly between different service providers, just like standard Simple Mail Transfer Protocol email does now for store-and-forward email service. From a technical perspective, it is an application layer communication protocol for federated real-time communication. It provides HTTP APIs and open source reference implementations for securely distributing and persisting messages in JSON format over an open federation of servers. It can integrate with standard web services via WebRTC, facilitating browser-to-browser applications. The Matrix standard specifies RESTful HTTP APIs for securely transmitting and replicating JSON data between Matrix-capable clients, servers and services. Clients send data by PUTting it to a ‘room’ on their server, which then replicates the data over all the Matrix servers participating in this ‘room’. This data is signed using a git-style signature to mitigate tampering, and the federated traffic is encrypted with HTTPS and signed with each server’s private key to avoid spoofing. Replication follows eventual consistency semantics, allowing servers to function even if offline or after data-loss by resynchronizing missing history from other participating servers. The Olm library provides for optional end-to-end encryption on a room-by-room basis via a Double Ratchet Algorithm implementation. It can ensure that conversation

data at rest is only readable by the room participants. With it configured, data transmitted over Matrix is only visible as ciphertext to the Matrix servers, and can be decrypted only by authorized participants in the room. The Olm and Megolm (an expansion of Olm to better suit the need for bigger rooms) libraries have been subject of a cryptographic review by NCC Group, whose findings are publicly available. The review was sponsored by the Open Technology Fund. Further technical and historical research has to analyze links and differences between the Echo Protocol and if Matrix is a technical subset of the Echo, deriving also timely later from it.

Matryoshka Doll

Matryoshka dolls (Russian: матрёшка), also known as Russian nesting dolls, stacking dolls, or Russian dolls, are the set of wooden dolls of decreasing size placed one inside another. The name "matryoshka" (матрёшка), literally "little matron", is a diminutive form of Russian female first name "Matryona" (Матрёна) or "Matriosha". A set of matryoshkas consists of a wooden figure, which separates, top from bottom, to reveal a smaller figure of the same sort inside, which has, in turn, another figure inside of it, and so on. The first Russian nested doll set was made in 1890 by Vasily Zvyozdochkin from a design by Sergey Malyutin, who was a folk crafts painter at Abramtsevo. Traditionally the outer layer is a woman, dressed in a sarafan, a long and shapeless traditional Russian peasant jumper dress. The figures inside may be of either gender; the smallest, innermost doll is typically a baby turned from a single piece

of wood. Much of the artistry is in the painting of each doll, which can be very elaborate. The dolls often follow a theme; the themes may vary, from fairy tale characters to Soviet leaders. In the west, Matryoshka dolls are often erroneously referred to as "babushka dolls", babushka meaning "grandmother" or "old woman". Matryoshka dolls are a traditional representation of the mother carrying a child within her and can be seen as a representation of a chain of mother's carrying on the family legacy through the child in their womb. Furthermore, Matryoshka dolls are used to illustrate the unity of body, soul, mind, heart and spirit. Matryoshkas are also used metaphorically, as a design paradigm, known as the "matryoshka principle" or "nested doll principle". It denotes a recognizable relationship of "object-within-similar-object" that appears in the design of many other natural and crafted objects. The onion metaphor is of similar character. If the outer layer is peeled off an onion, a similar onion exists within. This structure is employed by designers in applications such as the layering of clothes or the design of tables, where a smaller table nests within a larger table, and a smaller one within that. The layered framework is often used as approach for (multiple) encryption or network processes.



Figure 47: Matryoshka dolls set in a row [CC-SA3]

McEliece Algorithm

In cryptography, the McEliece cryptosystem is an asymmetric encryption algorithm developed in 1978 by Robert McEliece. It was the first such scheme to use randomization in the encryption process. The algorithm has currently not gained much acceptance in the cryptographic community but is a candidate for “post-quantum cryptography”, as it is immune to attacks using Shor’s algorithm and — more generally — measuring cost states using Fourier sampling. The recommended parameter sizes for the used Goppa code - which maximizes the adversary’s work factor - appears to be $n = 1024$, $t = 38$, and $k = 644$. The Niederreiter cryptosystem is a variation of the McEliece cryptosystem. The McEliece algorithm is

implemented open source in the Spot-On Encryption Suite, which is regarded as the first McEliece Messenger; and the Smoke Crypto Chat Messenger was the first messenger with the McEliece algorithm for mobile devices.

McNoodle Library

McNoodle is an open source library for McEliece asymmetric encryption. The implementation is based on the PKC Calculator by Marek Repka. Other reference papers are in the source included (papers.d). Divisions by zero may occur. (If this is a concern, please see `mcnoodle_private_key:: mcnoodle_private_key()` and adjust the generator-discovery algorithm). The library has been tested on Debian AMD 64-bit, Debian ARM 32-bit, Debian PowerPC 32-bit, FreeBSD 32-bit, and Windows 7 with Cygwin. Repositories under: <https://github.com/textbrowser/mcnoodle>.

Measurement

Measurement is the assignment of a number to a characteristic of an object or event, which can be compared with other objects or events. The scope and application of measurement are dependent on the context and discipline.

Media Bias

Media bias is the bias or perceived bias of journalists and news producers within the mass media in the selection of

events and stories that are reported and how they are covered. The term "media bias" implies a pervasive or widespread bias contravening the standards of journalism, rather than the perspective of an individual journalist or article. The direction and degree of media bias in various countries is widely disputed. Practical limitations to media neutrality include the inability of journalists to report all available stories and facts, and the requirement that selected facts be linked into a coherent narrative. Government influence, including overt and covert censorship, biases the media in some countries, for example China, North Korea and Myanmar. Market forces that result in a biased presentation include the ownership of the news source, concentration of media ownership, the selection of staff, the preferences of an intended audience, and pressure from advertisers. There are a number of national and international watchdog groups that report on bias in the media, even for news on cryptography.

MELODICA - Multi Encrypted Long Distance Calling

With the MELODICA feature in GoldBug Secure Messenger the user calls the friend cryptographically and sends a new end-to-end encrypting Gemini (AES-256-Key). The Key is sent over your asymmetric encryption of the RSA key. This is a secure way, as all other plaintext transfers like: email, spoken over phone or in other messengers, have to be regarded as unsafe and recorded. MELODICA stands for: Multi Encrypted Long Distance Calling. The idea is to call a friend even over a long distance of the Echo protocol and

exchange over secure asymmetric encryption a Gemini (AES-256 key) to establish an end-to-end encrypted channel. The MELODICA button was a graphical symbol for the beginning of the implementations for and development of Cryptographic Calling.

Mesh Networking

A mesh network (or simply meshnet) is a local network topology in which the infrastructure nodes (i.e. bridges, switches and other infrastructure devices) connect directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data from/to clients. This lack of dependency on one node allows for every node to participate in the relay of information. Mesh networks dynamically self-organize and self-configure, which can reduce installation overhead. The ability to self-configure enables dynamic distribution of workloads, particularly in the event that a few nodes should fail. This in turn contributes to fault-tolerance and reduced maintenance costs. Mesh topology may be contrasted with conventional star/tree local network topologies in which the bridges/switches are directly linked to only a small subset of other bridges/switches, and the links between these infrastructure neighbors are hierarchical. A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. It is also a form of wireless ad hoc network. A mesh refers to rich interconnection among devices or nodes. Wireless mesh networks often consist of mesh clients, mesh routers and gateways.

Mobility of nodes is less frequent. If nodes constantly or frequently move, the mesh spends more time updating routes than delivering data. In a wireless mesh network, topology tends to be more static, so that routes computation can converge and delivery of data to their destinations can occur. Hence, this is a low-mobility centralized form of wireless ad hoc network. Examples: (1) The Better Approach To Mobile Adhoc Networking (B.A.T.M.A.N.) is a routing protocol for multi-hop mobile ad hoc networks which is under development by the German "Freifunk" community and intended to replace the Optimized Link State Routing Protocol (OLSR). B.A.T.M.A.N.'s crucial point is the decentralization of the knowledge about the best route through the network — no single node has all the data. This technique eliminates the need to spread information concerning network changes to every node in the network. The individual node only saves information about the "direction" it received data from and sends its data accordingly. The data gets passed on from node to node and packets get individual, dynamically created routes. A network of collective intelligence is created. (2) An Echo Network can be considered as a Mesh Network. (3) FabFi is an open-source, city-scale, wireless mesh networking system. It is an inexpensive framework for sharing wireless internet from a central provider across a town or city. It was developed originally by FabLab, Jalalabad to provide high-speed internet. It is also designed for high performance across multiple hops.

Meta-Data

Metadata is data [information] that provides information about other data. Many distinct types of metadata exist, among these descriptive metadata, structural metadata, administrative metadata, reference metadata and statistical metadata. In the Internet meta data often refers to the recording of when how many data has been accessed or transferred by whom to whom.

MITM – [Hu]Man-in-the-middle Attack

(Not to be confused with Meet-in-the-middle attack).

In cryptography and computer security, a [hu]man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted wireless access point (Wi-Fi) could insert themselves as a man-in-the-middle. As an attack that aims at circumventing mutual authentication, or lack thereof, an MITM attack can succeed only when the attacker can

impersonate each endpoint to their satisfaction as expected from the legitimate ends. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, TLS can authenticate one or both parties using a mutually trusted certificate authority. Suppose Alice wishes to communicate with Bob. Meanwhile, Mallory wishes to intercept the conversation to eavesdrop and optionally to deliver a false message to Bob. First, Alice asks Bob for his public key. If Bob sends his public key to Alice, but Mallory is able to intercept it, an MITM attack can begin. Mallory sends a forged message to Alice that purports to come from Bob, but instead includes Mallory's public key. Alice, believing this public key to be Bob's, encrypts her message with Mallory's key and sends the enciphered message back to Bob. Mallory again intercepts, deciphers the message using her private key, possibly alters it if she wants, and re-enciphers it using the public key she intercepted from Bob when he originally tried to send it to Alice. When Bob receives the newly enciphered message, he believes it came from Alice. There is the need for Alice and Bob to have some way to ensure that they are truly each using each other's public keys, rather than the public key of an attacker. Otherwise, such attacks are generally possible, in principle, against any message sent using public-key technology. A variety of techniques can help defend against MITM attacks. All cryptographic systems that are secure against MITM attacks provide some method of authentication for messages or the sender (e.g. by SMP, JPAKE and Juggerknots). For gender neutrality MITM has changed to "(hu)man-in-the-middle".

MITM - Meet-in-the-middle Attack

(Not to be confused with (Hu)Man-in-the-middle attack).

The meet-in-the-middle attack (MITM) is a generic space-time trade-off cryptographic attack against encryption schemes which rely on performing multiple encryption operations in sequence. The MITM attack is the primary reason why Double DES is not used and why a Triple DES key (168-bit) can be brute forced by an attacker with 2^{56} space and 2^{112} operations. When trying to improve the security of a block cipher, a tempting idea is to encrypt the data several times using multiple keys. One might think this doubles or even n-tuples the security of the multiple-encryption scheme, depending on the number of times the data is encrypted, because an exhaustive search on all possible combination of keys (simple brute-force) would take $2^{n \cdot k}$ attempts if the data is encrypted with k-bit keys n times. The MITM is a generic attack which weakens the security benefits of using multiple encryptions by storing intermediate values from the encryptions or decryptions and using those to improve the time required to brute force the decryption keys. This makes a Meet-in-the-Middle attack (MITM) a generic space-time trade-off cryptographic attack. The MITM attack attempts to find the keys by using both the range (ciphertext) and domain (plaintext) of the composition of several functions (or block ciphers) such that the forward mapping through the first functions is the same as the backward mapping (inverse image) through the last functions, quite literally meeting in the middle of the composed function. For example, although Double DES encrypts the data with two different 56-bit keys, Double

DES can be broken with 2^{57} encryption and decryption operations.

Mix Network

Mix networks are routing protocols that create hard-to-trace communications by using a chain of proxy servers known as mixes which take in messages from multiple senders, shuffle them, and send them back out in random order to the next destination (possibly another mix node). This breaks the link between the source of the request and the destination, making it harder for eavesdroppers to trace end-to-end communications. Furthermore, mixes only know the node that it immediately received the message from, and the immediate destination to send the shuffled messages to, making the network resistant to malicious mix nodes. Each message is encrypted to each proxy using public key cryptography; the resulting encryption is layered like a Russian doll (except that each "doll" is of the same size) with the message as the innermost layer. Each proxy server strips off its own layer of encryption to reveal where to send the message next. If all but one of the proxy servers are compromised by the tracer, intractability can still be achieved against some weaker adversaries.

Monitoring

Monitoring is in general determining the status of a system, a process or an activity. Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network

administrator (via email, SMS or other alarms) in case of outages or other trouble. Network monitoring is part of network management.

Moore's Law

Moore's law is the observation that the number of transistors in a dense integrated circuit doubles about every two years. The observation is named after Gordon Moore, the co-founder of Fairchild Semiconductor and CEO of Intel, whose 1965 paper described a doubling every year in the number of components per integrated circuit and projected this rate of growth would continue for at least another decade. In 1975, looking forward to the next decade, he revised the forecast to doubling every two years. The period is often quoted as 18 months because of a prediction by Intel executive David House (being a combination of the effect of more transistors and the transistors being faster). Moore's prediction proved accurate for several decades and has been used in the semiconductor industry to guide long-term planning and to set targets for research and development. Moore's law is an observation and projection of a historical trend and not a physical or natural law.

Mosaic

A mosaic is the name for a file splitted into smaller parts. These smaller parts are commonly called "blocks", "parts" or "chunks", in the Spot-On encryption application they are

called: “links”. All links build the mosaic, which can be assembled to the file, which has been transferred.

Multi-Encryption

Multiple encryption is the process of encrypting an already encrypted message one or more times, either using the same or a different algorithm. It is also known as cascade encryption, cascade ciphering, multiple encryption, and superencipherment. Superencryption refers to the outer-level encryption of a multiple encryption. A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. A hybrid cryptosystem can be constructed using any two separate cryptosystems: first, a key encapsulation scheme, which is a public-key cryptosystem, and second a data encapsulation scheme, which is a symmetric-key cryptosystem. Perhaps the most commonly used hybrid cryptosystems are the OpenPGP (RFC 4880) file format and the PKCS #7 (RFC 2315) file format, both used by many different systems. Multiple encryption is the process of encrypting an already encrypted message one or more times, either using the same or a different algorithm. Multiple encryption (Cascade Ciphers) reduces the consequences in the case that our favorite cipher is already broken and is continuously exposing our data without our knowledge. When a cipher is broken (something we will not know), the use of other ciphers may represent the only security in the system. Since we cannot scientifically prove that any particular cipher is strong, the question is not whether subsequent

ciphers are strong, but instead, what would make us believe that any particular cipher is so strong as to need no added protection. Folk Theorem: A cascade of ciphers is at least as difficult to break as any of its component ciphers. When a cipher is broken (something we will not know), the use of other ciphers may represent the only security in the system. Since we cannot scientifically prove that any particular cipher is strong, the question is not whether subsequent ciphers are strong, but instead, what would make us believe that any particular cipher is so strong as to need no added protection. The encryption clients GoldBug and Spot-On brought Multi-Encryption with(in) the Echo-Protocol forward.

Mutual Authentication

Mutual authentication or two-way authentication refers to two parties authenticating each other at the same time, being a default mode of authentication in some protocols (IKE, SSH) and optional in others (TLS). By default the TLS protocol only proves the identity of the server to the client using X.509 certificate and the authentication of the client to the server is left to the application layer. TLS also offers client-to-server authentication using client-side X.509 authentication. As it requires provisioning of the certificates to the clients and involves less user-friendly experience, it's rarely used in end-user applications. Mutual TLS authentication (mTLS) is much more widespread in business-to-business (B2B) applications, where a limited number of programmatic and homogeneous clients are connecting to specific web services, the operational burden

is limited, and security requirements are usually much higher as compared to consumer environments.

Neighbor

In graph theory, a neighbor of a vertex is another vertex that is connected to it by an edge.

Netcat

Netcat (often abbreviated to nc or Ncat) is a computer networking utility for reading from and writing to network connections using TCP or UDP. Netcat is designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts.

Neuland

Neuland is a German term within the context of the Internet and non-IT-savvy people, deriving as satirical designation in reference to the sentence of the year 2013 by German chancellor Angela Merkel, in which she commented on her U.S.-surveilled mobile phone: the internet is a “new territory” (aka Neuland) for all of us.

NIST - National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) is a physical sciences laboratory, and a non-regulatory

agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. NIST's activities are organized into laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement.

NOVA

NOVA describes a password on the to-be-transferred file. It is a symmetric encryption of the file scheduled for the transfer. It can be compared with the term of a GoldBug-Password on an e-mail. Both are technically created with an AES-256 (or a user-defined password).

NTL - Number Theory Library

NTL (Number Theory Library) is a C++ library for doing number theory. NTL supports arbitrary length integer and arbitrary precision floating point arithmetic, finite fields, vectors, matrices, polynomials, lattice basis reduction and basic linear algebra. NTL is free software released under the GNU General Public License.

NTRU

NTRU is a patented and open source public-key cryptosystem that uses lattice-based cryptography to encrypt and decrypt data. It consists of two algorithms:

NTRUEncrypt, which is used for encryption, and NTRUSign, which is used for digital signatures. Unlike other popular public-key cryptosystems, it is resistant to attacks using Shor's algorithm (i.e. by „Quantum Computing“) and its performance has been shown to be significantly better.

Null Cipher

A null cipher, also known as concealment cipher, is an ancient form of encryption where the plaintext is mixed with a large amount of non-cipher material. Today it is regarded as a simple form of steganography, which can be used to hide ciphertext. In classical cryptography, a null is intended to confuse the cryptanalyst. In a null cipher, the plaintext is included within the ciphertext and one needs to discard certain characters in order to decrypt the message. Most characters in such a cryptogram are nulls, only some are significant, and some others can be used as pointers to the significant ones. Here is an example implementation of a null cipher. Stringing together the first letter of every third word of the following covertext reveals "Wikipedia" as the hidden message: *It's important we allow anyone interested in gaining knowledge access to information which is published freely. There exists a website devoted to this idea, and you are on it!* In general, it is difficult and time-consuming to produce covertexts that seem natural and would not raise suspicion. If no key or actual encryption is involved, the security of the message relies entirely on the secrecy of the concealment method. Null ciphers in modern times are utilized by prison inmates in an

attempt to have their most suspicious messages pass inspection.

Number Theory

Number theory (or arithmetic or higher arithmetic in older usage) is a branch of pure mathematics devoted primarily to the study of the integers. German mathematician Carl Friedrich Gauss (1777–1855) said, "Mathematics is the queen of the sciences—and number theory is the queen of mathematics." Number theorists study prime numbers as well as the properties of objects made out of integers (for example, rational numbers) or defined as generalizations of the integers (for example, algebraic integers).



Figure 48: Carl Friedrich Gauss: “Mathematics is the queen of the sciences—and number theory is the queen of mathematics”. [PD]

OFFSystem

The Owner-Free File System (OFF System, or OFF for short) is a peer-to-peer distributed file system in which all shared files are represented by randomized multi-used data blocks. Instead of anonymizing the network, the data blocks are anonymized and therefore, only data garbage is ever exchanged and stored and no forwarding via intermediate nodes is required. The OFF System is a kind of anonymous, fully decentralized P2P file sharing program and network. In contrast to other anonymous file sharing networks, which derive their anonymity from forwarding their data blocks via intermediate network nodes, OFF derives its anonymity from anonymizing the data files. Within the OFFSystem, two files are XORed with a key into random data. Only with the right key the one or other file can be restored. They key is shared over the same P2P network as the XORed data blocks. By design the key needs to be shared over a web of trust friend-to-friend network, e.g. like in Freenet. It is found under: <http://sourceforge.net/projects/offsystem/>

OMEMO

OMEMO is an extension to the Extensible Messaging and Presence Protocol (XMPP, "Jabber") for multi-client end-to-end encryption. OMEMO uses the Double Ratchet Algorithm "to provide multi-end to multi-end encryption, allowing messages to be synchronized securely across multiple clients, even if some of them are offline". The name "OMEMO" is a recursive acronym for "OMEMO

Multi-End Message and Object Encryption". It is an open standard based on the Double Ratchet Algorithm and the Personal Eventing Protocol (PEP, XEP-0163). OMEMO offers future and forward secrecy and deniability with message synchronization and offline delivery.

Open Source

Open source is a term denoting that a product includes permission to use its source code, design documents, or content. It most commonly refers to the open-source model, in which open-source software or other products are released under an open-source license as part of the open-source-software movement. Use of the term originated with software but has expanded beyond the software sector to cover other open content and forms of open collaboration. In Cryptography only open source software allows everyone to proof that the code has no backdoors implemented.

OpenPGP - Open Pretty Good Privacy

The OpenPGP standard (also Pretty Good Privacy) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991. PGP and similar software follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data.

OpenSSH - Open Secure Shell

OpenSSH (also known as OpenBSD Secure Shell) is a suite of secure networking utilities based on the Secure Shell (SSH) protocol, which provides a secure channel over an unsecured network in a client–server architecture. OpenSSH started as a fork of the free SSH program developed by Tatu Ylönen; later versions of Ylönen's SSH were proprietary software offered by SSH Communications Security. OpenSSH was first released in 1999, and is currently developed as part of the OpenBSD operating system. OpenSSH is not a single computer program, but rather a suite of programs that serve as alternatives to unencrypted protocols like Telnet and FTP. OpenSSH is integrated into several operating systems, while the portable version is available as a package in other systems.

OpenSSL - Open Secure Sockets Layer

In computer networking, OpenSSL is a software library to be used in applications that need to secure communications against eavesdropping or need to ascertain the identity of the party at the other end. It has found wide use in internet web servers, serving a majority of all web sites. OpenSSL contains an open source implementation of the SSL and TLS protocols. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols designed to provide communications security over a computer network.

Opportunistic Encryption

Opportunistic encryption (OE) refers to any system that, when connecting to another system, attempts to encrypt the communications channel, otherwise falling back to unencrypted communications (e.g. over WPA3 defined by the Wi-Fi Alliance). This method requires no pre-arrangement between the two systems. Opportunistic encryption can be used to combat passive wiretapping. (An active wiretapper, on the other hand, can disrupt encryption negotiation to either force an unencrypted channel or perform a meet-in-the-middle attack on the encrypted link.) It does not provide a strong level of security as authentication may be difficult to establish and secure communications are not mandatory. However, it does make the encryption of most Internet traffic easy to implement, which removes a significant impediment to the mass adoption of Internet traffic security. Opportunistic encryption on the Internet is described in RFC 4322 "Opportunistic Encryption using the Internet Key Exchange (IKE)" and another version in RFC 7435 "Opportunistic Security: Some Protection Most of the Time". Opportunistic encryption can also be used for specific traffic like e-mail using the SMTP STARTTLS extension for relaying messages across the Internet, or the Internet Message Access Protocol (IMAP) STARTTLS extension for reading e-mail. With this implementation, it is not necessary to obtain a certificate from a certificate authority, as a self-signed certificate can be used. Many systems employ a variant with third-party add-ons to traditional email packages by first attempting to obtain an encryption key and if unsuccessful, then sending the email in the clear. In

practice, STARTTLS in SMTP is often deployed with self-signed certificates, which represents a minimal one-time task for a system administrator, and results in most email traffic being opportunistically encrypted.

OTM - One-Time-Magnet

A One-Time-Magnet (OTM) is a Magnet, which is deployed for the File-Transfer within the StarBeam-Function for file transfer. After sending the File using the cryptographic values included in the Magnet-Link, the Magnet is deleted within the Spot-On application. Other Magnets for the StarBeam-Function can be used several times – this means, several and different files can be transferred to the receiver through the symmetric channel (including all users, knowing the specific Magnet).

OTP - One-Time-Pad

In cryptography, the one-time pad (OTP) is an encryption technique that cannot be cracked if used correctly. In this technique, a plaintext is paired with a random secret key (also referred to as a one-time pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, is at least as long as the plaintext, is never reused in whole or in part, and is kept completely secret, then the resulting ciphertext will be impossible to decrypt or break.

OTR - Off-the-Record

Off-the-Record Messaging (OTR) is a cryptographic protocol that provides encryption for instant messaging conversations. OTR uses a combination of AES symmetric-key algorithm with 128 bits key length, the Diffie-Hellman key exchange with 1536 bits group size, and the SHA-1 hash function. These sizes are today outdated. In addition to authentication and encryption, OTR provides forward secrecy and malleable encryption.

Ozone Address Postbox

The Ozone Postbox is a way to reach offline friends within the Smoke Mobile Crypto Client respective the SmokeStack Communication Server for Android. The Ozone Postbox serves as a cache for friends, which are not online. The Ozone is just a passphrase string, which must be applied in both, the client Smoke and the Server SmokeStack. The rest is done by the cryptographic keys. The Ozone can be initialized within the client by using the dyndns or IP name, port and TCP, e.g.: dyndns.org:4711:TCP. If the server administrator of SmokeStack applies this string also as one Ozone within the server, the clients will automatically add the string as the Ozone when entering the IP respective dyndns-string of the server. An Ozone address may be assigned via the Settings activity. If an Ozone address is defined and the network is available, Smoke will request external messages once per minute. An Ozone address is a pseudo-private string which identifies a virtual entity. Smoke and SmokeStack utilize Ozones as a means of

retrieving and storing offline messages and public-key pairs. Smoke supports one Ozone while SmokeStack supports infinitely many. Ozone addresses must be exchanged separately. It is possible for multiple Smoke parties to house distinct Ozones if common SmokeStack instances are aware of the distinct Ozone addresses. Please note that public Ozone addresses will introduce denial of service vulnerabilities.

Padding

Padding refers to a number of distinct practices which all include adding data to the beginning, middle, or end of a message prior to encryption. In classical cryptography, padding may include adding nonsense phrases to a message to obscure the fact that many messages end in predictable ways, e.g. sincerely yours. Official messages often start and end in predictable ways: My dear ambassador, Weather report, Sincerely yours, etc. The primary use of padding with classical ciphers is to prevent the cryptanalyst from using that predictability to find known plaintext that aids in breaking the encryption. Random length padding also prevents an attacker from knowing the exact length of the plaintext message. A famous example of classical padding which caused a great misunderstanding is "the world wonders" incident, which nearly caused an Allied loss at the WWII Battle off Samar, part of the larger Battle of Leyte Gulf. In that example, Admiral Chester Nimitz, the Commander in Chief, U.S. Pacific Fleet in World War II, sent the following message to Admiral Bull Halsey, commander of Task Force Thirty Four

(the main Allied fleet) at the Battle of Leyte Gulf, on October 25, 1944: Where is, repeat, where is Task Force Thirty Four? With padding (bolded) and metadata added, the message became: TURKEY TROTS TO WATER GG FROM CINCPAC ACTION COM THIRD FLEET INFO COMINCH CTF SEVENTY-SEVEN X WHERE IS RPT WHERE IS TASK FORCE THIRTY FOUR RR THE WORLD WONDERS. Halsey's radio operator mistook some of the padding for the message, so Admiral Halsey ended up reading the following message: Where is, repeat, where is Task Force Thirty Four? The world wonders. Admiral Halsey interpreted the padding phrase "the world wonders" as a sarcastic reprimand, causing him to have an emotional outburst and then lock himself in his bridge and sulk for an hour before moving his forces to assist at the Battle off Samar. Halsey's radio operator should have been tipped off by the letters RR that "the world wonders" was padding; all other radio operators who received Admiral Nimitz's message correctly removed both padding phrases. Many classical ciphers arrange the plaintext into particular patterns (e.g., squares, rectangles, etc.) and if the plaintext doesn't exactly fit, it is often necessary to supply additional letters to fill out the pattern. Using nonsense letters for this purpose has a side benefit of making some kinds of cryptanalysis more difficult.

Pandamonium

Pandamonium is a Web-Crawler written in C++, with which URLs of a domain or website can be indexed for Spot-On's function of an URL database. The Pandamonium Web Crawler can allocate for the URL-Search function within the

Spot-On Encryption Suite a bunch of URLs over the Import-function.

Passphrase

A passphrase is a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage but is generally longer for added security. Passphrases are often used to control both access to, and operation of, cryptographic programs and systems. Passphrases are particularly applicable to systems that use the passphrase as an encryption key. The origin of the term is by analogy with password. E.g. the passphrase in Spot-On must be at least 16 characters long, this is used to create a cryptographic hash, which more secure by a such defined passphrase.

Pass-through

The Pass-through method within the application Spot-On describes a function for a network path from an application, e.g. a Gopher client, over two Spot-On instances to another Gopher Client: Gopher -> Spot-On -> Internet -> Spot-On – Gopher. This function works similar as a VPN tunnel or a proxy for the external application. As the connection from a Spot-On node over the Internet to another Spot-On node is encrypted, also e.g. with the McEliece algorithm, even old applications with no encryption can communicate now secure over the Internet. The application to tie in must only meet some tolerance for

chaotic transmission, a Gopher client can be ideal used for such tests.

Password

A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which is to be kept secret from those not allowed access. In modern times, usernames and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc.

Patch-Points

Patch-Points describe the entry- and end-nodes of the pass-through functionality. This functionality of has been discussed in the Spot-On Developer Forum originally as Patch-Points, has then be named within the application as pass-through function. At Patch-Points two older applications without encryption can communicate over the secure localhost connection of two connected Spot-On nodes.

Pegasus Spyware

Pegasus is a spyware that can be installed on devices running certain versions of iOS, Apple's mobile operating

system, developed by the Israeli cyberarms firm, NSO Group. Discovered in August 2016 after a failed attempt at installing it on an iPhone belonging to a human rights activist, an investigation revealed details about the spyware, its abilities, and the security vulnerabilities it exploited. Pegasus is capable of reading text messages, tracking calls, collecting passwords, tracing the location of the phone, and gathering information from apps. News of the spyware garnered significant media attention. It was called the "most sophisticated" smartphone attack ever. This hidden mobile application grabs entered text as plaintext before it is encrypted and sent. That's why "Going the Extra Mile" is important with typing on a device, that has never been connected to the Internet for updates, and sends out the encrypted packet e.g. over a Bluetooth connection to another Internet connected device.

Pepper

A pepper is a secret added to an input such as a password prior to being hashed with a cryptographic hash function. As of 2017, NIST recommends using a secret input when storing memorized secrets such as passwords. A pepper performs a comparable role to a salt, but while a salt is not secret (merely unique) and can be stored alongside the hashed output, a pepper is secret and must not be stored with the output. The hash and salt are usually stored in a database, but a pepper must be stored separately (e.g. in a configuration file) to prevent it from being obtained by the attacker in case of a database breach. Where the salt only has to be long enough to be unique, a pepper has to be

secure to remain secret (at least 112 bits is recommended by NIST), otherwise an attacker only needs one known entry to crack the pepper. Finally, the pepper must be generated anew for every application it is deployed in, otherwise a breach of one application would result in lowered security of another application. A pepper adds security to a database of salts and hashes because unless the attacker is able to obtain the pepper, they cannot crack a single hash, no matter how weak the original password. If a strong hashing algorithm is not selected, an attacker can brute force the hashes and recover weak passwords. The encryption equivalent of a pepper is the encryption key. By including pepper in the hash, one can have the advantages of both methods: uncrackable passwords so long as the pepper remains unknown to the attacker, and even in the case the pepper is breached, an attacker still has to crack the hashes. For comparison, when encrypting passwords, anyone with knowledge of the encryption key (including system administrators) can instantly decrypt all passwords; hence, it is always recommended to hash passwords instead of encrypting them, even when not using a pepper.

Performance

Performance is a measurable result. Note: Performance can relate either to quantitative or qualitative findings.

PGP

See OpenPGP.

Pigeonhole Principle

The pigeonhole principle states that if n items are put into m containers, with $n > m$, then at least one container must contain more than one item. This theorem is exemplified in real life by truisms like: in any group of three gloves there must be at least two left gloves or at least two right gloves.



Figure 49: Pigeon Principle [SA3]

Pigeons in holes. Here there are $n = 10$ pigeons in $m = 9$ holes. Since 10 is greater than 9, the pigeonhole principle says that at least one hole has more than one pigeon.

It is an example of a counting argument. This seemingly obvious statement can be used to demonstrate possibly unexpected results; for example, that there must be (at

least) two people in London who have the same number of hairs on their heads. The first formalization of the idea is believed to have been made by Peter Gustav Lejeune Dirichlet in 1834 under the name Schubfachprinzip ("drawer principle" or "shelf principle", *ibid*). For this reason, it is also commonly called Dirichlet's box principle or Dirichlet's drawer principle. The principle has several generalizations and can be stated in various ways. Though the most straightforward application is to finite sets (such as pigeons and boxes), it is also used with infinite sets that cannot be put into one-to-one correspondence. To do so requires the formal statement of the pigeonhole principle, which is: there does not exist an injective function whose codomain is smaller than its domain.

PKI - Public Key Infrastructure

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred. Hence, in cryptography, a PKI is an arrangement that binds public keys with respective identities of entities (like people and organizations). The binding is established through a process

of registration and issuance of certificates at and by a certificate authority (CA). Depending on the assurance level of the binding, this may be carried out by an automated process or under human supervision.

Plaintext

Plaintext or cleartext is unencrypted information, as opposed to information encrypted for storage or transmission. Plaintext usually means unencrypted information pending input into cryptographic algorithms, usually encryption algorithms. Cleartext usually refers to data that is transmitted or stored 'in the clear'. With the advent of computing, the term plaintext expanded beyond human-readable documents to mean any data, including binary files, in a form that can be viewed or used without requiring a key or other decryption device. Information - a message, document, file, etc. - if to be communicated or stored in encrypted form is referred to as plaintext. Plaintext is used as input to an encryption algorithm; the output is usually termed ciphertext, particularly when the algorithm is a cipher. Codetext is less often used, and almost always only when the algorithm involved is actually a code. Some systems use multiple layers of encryption, with the output of one encryption algorithm becoming „Plaintext“-input for the next. Insecure handling of plaintext can introduce weaknesses into a cryptosystem by letting an attacker bypass the cryptography altogether. Plaintext is vulnerable in use and in storage, whether in electronic or paper format.

Plausible Deniability

Plausible deniability is the ability of people (typically senior officials in a formal or informal chain of command) to deny knowledge of or responsibility for any damnable actions committed by others in an organizational hierarchy because of a lack of evidence that can confirm their participation, even if they were personally involved in or at least willfully ignorant of the actions. In the case that illegal or otherwise disreputable and unpopular activities become public, high-ranking officials may deny any awareness of such acts to insulate themselves and shift blame onto the agents who carried out the acts, as they are confident that their doubters will be unable to prove otherwise. The lack of evidence to the contrary ostensibly makes the denial plausible, that is, credible, although sometimes it merely makes it unactionable. The term typically implies forethought, such as intentionally setting up the conditions to plausibly avoid responsibility for one's (future) actions or knowledge. In some organizations, legal doctrines such as command responsibility exist to hold major parties responsible for the actions of subordinates involved in heinous acts and nullify any legal protection that their denial of involvement would carry. In cryptography, deniable encryption may be used to describe steganographic techniques, where the very existence of an encrypted file or message is deniable in the sense that an adversary cannot prove that an encrypted message exists. In this case the system is said to be 'fully undetectable' (FUD). Some systems take this further, such as MaruTukku, FreeOTFE and (to a much lesser extent) TrueCrypt and VeraCrypt, which nest encrypted data. The owner of the

encrypted data may reveal one or more keys to decrypt certain information from it, and then deny that more keys exist, a statement which cannot be disproven without knowledge of all encryption keys involved. The existence of "hidden" data within the overtly encrypted data is then deniable in the sense that it cannot be proven to exist. Hence, in cryptography and steganography, plausibly deniable encryption describes encryption techniques where the existence of an encrypted file or message is deniable in the sense that an adversary cannot prove that the plaintext data exists. The users may convincingly deny that a given piece of data is encrypted, or that they are able to decrypt a given piece of encrypted data, or that some specific encrypted data exists. Such denials may or may not be genuine. For example, it may be impossible to prove that the data is encrypted without the cooperation of the users. If the data is encrypted, the users genuinely may not be able to decrypt it. Deniable encryption serves to undermine an attacker's confidence either that data is encrypted, or that the person in possession of it can decrypt it and provide the associated plaintext.

Point-to-Point

In telecommunications, a point-to-point connection refers to a communications connection between two communication endpoints or nodes. An example is a telephone call, in which one telephone is connected with one other, and what is said by one caller can only be heard by the other. This is contrasted with a point-to-multipoint

or broadcast connection, in which many nodes can receive information transmitted by one node.

Policy

A policy covers intentions and direction of a formal entity as formally expressed by its management. Hence, a policy is a deliberate system of principles to guide decisions and achieve rational outcomes. A policy is a statement of intent, and is implemented as a procedure or protocol. Policies are generally adopted by a governance body within an organization. Policies can assist in both subjective and objective decision making. Policies to assist in subjective decision making usually assist senior management with decisions that must be based on the relative merits of a number of factors, and as a result are often hard to test objectively, e.g. work-life balance policy. In contrast policies to assist in objective decision making are usually operational in nature and can be objectively tested, e.g. password policy.

POP3 - Post Office Protocol

In computing, the Post Office Protocol (POP or POP3) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection. POP has been developed through several versions, with version 3 (POP3) being the last standard in common use.

POPTASTIC

POPTASTIC is a function, which enables encrypted chat and encrypted e-mail over the regular POP3 and IMAP-Postboxes of a user. The Spot-On Encryption Suite recognizes automatically, if the message has to be regarded as a chat-message or an e-mail-message. For that, the POPTASTIC encryption key is used. Once with a friend exchanged, this key is sending all e-mails between to e-mail-partner only as encrypted e-mail. Third, POPTASTIC enables – respective the insertion of the POP3 / IMAP account information into the settings enables – also an old-fashioned and unencrypted E-mail-communication to @-E-mail-Addresses. Spot-On extends the Instant Messaging with this function to a regular e-mail-client and also to an always encrypting e-mail-client over the POPTASTIC Key. The e-mail-addresses for encrypted e-mails are indicated with a lock icon. Encrypted Chat is enabled over the free ports for e-mail also behind more restrictive hardware environments at any time.

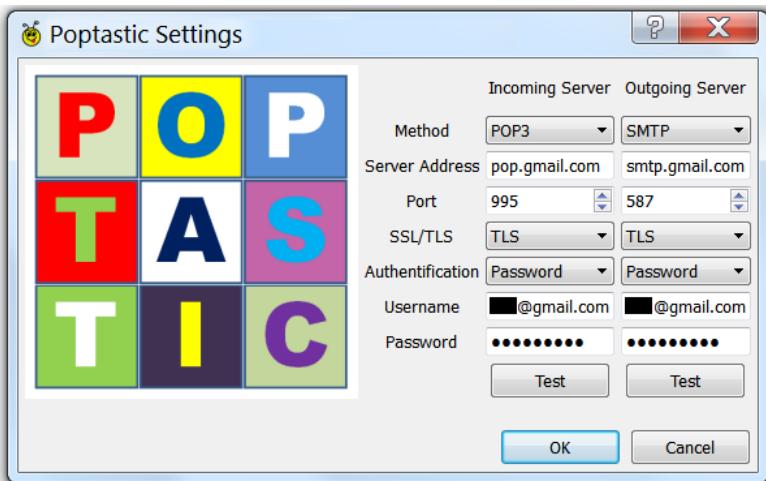


Figure 50: Settings within an application using e-mail-Servers for Chat over the POPTASTIC Protocol [PD]

The POPTASTIC Protocol has been released with GoldBug V 1.7 (2014-12-06) "POPTASTIC-XMAS-Release: Encrypted chat over POP3: Use IMAP&POP3 Servers for Chat" (<https://sourceforge.net/p/goldbug/wiki/release-history/>) while POPTASTIC within DeltaChat started with a first commit two years later in 2016, referenced to PGP and IMAP.

PostgreSQL

PostgreSQL, often simply Postgres, is an object-relational database management system (ORDBMS) with an emphasis on extensibility and standards-compliance. As a database server, its primary function is to store data securely, supporting best practices, and to allow for retrieval at the request of other software applications. It can handle workloads ranging from small single-machine applications to large Internet-facing applications with many concurrent

users. PostgreSQL implements the majority of the SQL:2011 standard.

Post-Quantum Cryptography

Post-quantum cryptography is distinct from quantum cryptography, which refers to using quantum phenomena to achieve secrecy and detect eavesdropping. Post-quantum cryptography (sometimes referred to as quantum-proof, quantum-safe or quantum-resistant) refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against an attack by a quantum computer. As of 2018, this is not true for the most popular public-key algorithms, which can be efficiently broken by a sufficiently strong hypothetical quantum computer. The problem with currently popular algorithms is that their security relies on one of three hard mathematical problems: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem. All of these problems can be easily solved on a sufficiently powerful quantum computer running Shor's algorithm. Even though current, publicly known, experimental quantum computers lack processing power to break any real cryptographic algorithm, many cryptographers are designing new algorithms to prepare for a time when quantum computing becomes a threat. This work has gained greater attention from academics and industry through the PQCrypto conference series since 2006 and more recently by several workshops on Quantum Safe Cryptography hosted by the European Telecommunications Standards Institute (ETSI) and the

Institute for Quantum Computing. Currently post-quantum cryptography research is mostly focused on six different approaches: (1) Lattice-based cryptography, (2) Multivariate cryptography, (3) Hash-based cryptography, (4) Code-based cryptography, (5) Supersingular elliptic curve isogeny cryptography, (6) Symmetric key quantum resistance. In contrast to the threat quantum computing poses to current public-key algorithms, most current symmetric cryptographic algorithms and hash functions are considered to be relatively secure against attacks by quantum computers. Doubling the key size can in some cases effectively block attacks. Thus post-quantum symmetric cryptography does not need to differ significantly from current symmetric cryptography.

PRISM (Surveillance Program)

PRISM is a code name for a program under which the United States National Security Agency (NSA) collects Internet communications from various US Internet companies. PRISM collects stored Internet communications based on demands made to Internet companies such as Google LLC to turn over any data that match court-approved search terms. The NSA can use these PRISM requests for plaintext to target communications that were encrypted when they traveled across the Internet backbone, to focus on stored data that telecommunication filtering systems discarded earlier, and to get data that is easier to handle, among other things.

Privacy

Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals but share common themes. When something is private to a person, it usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps with security (confidentiality), which can include the concepts of appropriate use, as well as protection of information. Privacy may also take the form of bodily integrity. The right not to be subjected to unsanctioned invasions of privacy by the government, corporations or individuals is part of many countries' privacy laws, and in some cases, constitutions. All countries have laws which in some way limit privacy. An example of this would be law concerning taxation, which normally requires the sharing of information about personal income or earnings. In some countries individual privacy may conflict with freedom of speech laws and some laws may require public disclosure of information which would be considered private in other countries and cultures. The right to privacy is an element of various legal traditions to restrain governmental and private actions that threaten the privacy of individuals. Over 150 national constitutions mention the right to privacy. Since the global surveillance disclosures of 2013, initiated by ex-NSA employee Edward Snowden, the inalienable human right to privacy has been a subject of international debate. Internet privacy involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and

displaying of information pertaining to oneself via the Internet. Internet privacy is a subset of data privacy. Privacy concerns have been articulated from the beginnings of large-scale computer sharing. The distinction or overlap between secrecy and privacy is ontologically subtle, which is why the word „Privacy“ is an example of an untranslatable lexeme, and many languages do not have a specific word for „Privacy“. Such languages either use a complex description to translate the term (such as Russian combining the meaning of *удединение*—solitude, *секретность*—secrecy, and *частная жизнь*—private life) or borrow from English „Privacy“ (as Indonesian *privasi* or Italian *la privacy*). The distinction hinges on the discreteness of interests of parties (persons or groups), which can have emic variation depending on cultural mores of individualism, collectivism, and the negotiation between individual and group rights. The difference is sometimes expressed humorously as, "when I withhold information, it is privacy; when you withhold information, it is secrecy."



Figure 51: Privacy may be lessened by surveillance – in this case through CCTV [SA3]

Privacy Amplification

Privacy amplification is a method for reducing (and effectively eliminating) Eve's partial information about Alice and Bob's key. This partial information could have been

gained both by eavesdropping on the quantum channel during key transmission (thus introducing detectable errors), and on the public channel during information reconciliation (where it is assumed Eve gains all possible parity information). Privacy amplification uses Alice and Bob's key to produce a new, shorter key, in such a way that Eve has only negligible information about the new key. This can be done using a universal hash function, chosen at random from a publicly known set of such functions, which takes as its input a binary string of length equal to the key and outputs a binary string of a chosen shorter length. The amount by which this new key is shortened is calculated, based on how much information Eve could have gained about the old key (which is known due to the errors this would introduce), in order to reduce the probability of Eve having any knowledge of the new key to a very low value. As an example of privacy amplification: in Smoke Crypto Messenger the Sip-Hash ID or Aliase-String defines is a new encrypted channel from Alice to Bob to protect the public key.

Private Key

Public-key cryptography refers to a set of cryptographic algorithms that are based on mathematical problems that currently admit no efficient solution. The strength lies in the “impossibility” (computational impracticality) for a properly generated private key to be determined from its corresponding public key. Thus the public key may be published without compromising security. Security depends only on keeping the private key private; e.g. to prevent an

upload of the private key especially on mobile operating systems. Hence, the private key should be stored encrypted on the device.

Private Servers

The Communication Server SmokeStack supports the concept of private servers for TCP clients. A private server will read and write data if and only if a remote peer has been authenticated. The authentication process is as follows with four steps: 1. A private server generates a 64-byte stream of random data and concatenates the bytes with the current system time. 2. The server submits the SHA-512 hash of the information generated in the previous step to the remote peer after the SSL/TLS handshake has been completed. 3. A remote peer digitally signs the stream of data and submits the digital signature to the remote server. 4. The remote server inspects the digital signature. If the signature is valid, the remote peer is authenticated. A private server is defined after the desired participants have been completely defined in SmokeStack.

Pseudorandom Number Generator

A pseudorandom number generator (PRNG), also known as a deterministic random bit generator (DRBG), is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers. The PRNG-generated sequence is not truly random, because it is completely determined by an initial value, called the PRNG's seed (which may include

truly random values). Although sequences that are closer to truly random can be generated using hardware random number generators, pseudorandom number generators are important in practice for their speed in number generation and their reproducibility. PRNGs are central in applications such as simulations and electronic games. Good statistical properties are a central requirement for the output of a PRNG. In general, careful mathematical analysis is required to have any confidence that a PRNG generates numbers that are sufficiently close to random to suit the intended use. John von Neumann cautioned about the misinterpretation of a PRNG as a truly random generator, and joked that "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin." Cryptographic applications require the output not to be predictable from earlier outputs, and more elaborate algorithms, which do not inherit the linearity of simpler PRNGs, are needed.

Public Key Certificate

A public key certificate, also known as a digital certificate or identity certificate, is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject. In email encryption, code signing, and e-signature

systems, a certificate's subject is typically a person or organization. However, in Transport Layer Security (TLS) a certificate's subject is typically a computer or other device, though TLS certificates may identify organizations or individuals in addition to their core role in identifying devices. In a typical public-key infrastructure (PKI) scheme, the certificate issuer is a certificate authority (CA), usually a company that charges customers to issue certificates for them. By contrast, in a web of trust scheme, individuals sign each other's keys directly, in a format that performs a similar function to a public key certificate. The most common format for public key certificates is defined by X.509. Because X.509 is very general, the format is further constrained by profiles defined for certain use cases, such as Public Key Infrastructure (X.509) as defined in RFC 5280.

Public Key Cryptography

Public-key cryptography refers to a set of cryptographic algorithms that are based on mathematical problems that currently admit no efficient solution – particularly those inherent in certain integer factorization, discrete logarithm, and elliptic curve relationships. It is computationally easy for a user to generate a public and private key-pair and to use it for encryption and decryption. The strength lies in the “impossibility” (computational impracticality) for a properly generated private key to be determined from its corresponding public key. Thus the public key may be published without compromising security. Security depends especially on keeping the private key private.

PURE-FS - Pure Forward Secrecy

Pure Forward Secrecy refers to a communication in the e-mail function of Spot-On, within which the information is not sent over asymmetrical keys, but over temporary, ephemeral keys, which generate a symmetric encryption. The ephemeral keys for Pure Forward Secrecy are exchanged over asymmetric keys, but then the message is sent exclusively over the temporary symmetric key. Compare in a different approach of Instant Perfect Forward Secrecy, that the messages is encrypted and transferred with both, a symmetric key and also with a asymmetric key within the format of the Echo-protocol.

P2P - Peer-to-Peer

Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.

Qt

Qt is a cross-platform application framework that is widely used for developing application software that can be run on various software and hardware platforms with little or no

change in the underlying codebase, while still being a native application with the capabilities and speed thereof. Qt is currently being developed both by the Qt Company, a subsidiary of Digia, and the Qt Project under open source governance, involving individual developers and firms working to advance Qt.

Quantum Computing

Quantum computing is the use of quantum-mechanical phenomena such as superposition and entanglement to perform computation. A quantum computer is used to perform such computation, which can be implemented theoretically or physically. The field of Quantum Computing is actually a sub-field of quantum information science, which includes quantum cryptography and quantum communication. Quantum Computing was started in the early 1980s when Richard Feynman and Yuri Manin expressed the idea that a quantum computer had the potential to simulate things that a classical computer could not. In 1994, Peter Shor shocked the world with an algorithm that had the potential to decrypt all secured communications.

Quantum Cryptography

Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best-known example of quantum cryptography is quantum key distribution which offers an information-theoretically secure solution to the key exchange problem.

The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication. For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed (no-cloning theorem). This could be used to detect eavesdropping in quantum key distribution. The most well-known and developed application of quantum cryptography is quantum key distribution (QKD), which is the process of using quantum communication to establish a shared key between two parties (Alice and Bob, for example) without a third party (Eve) learning anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob. If Eve tries to learn information about the key being established, discrepancies will arise causing Alice and Bob to notice. Once the key is established, it is then typically used for encrypted communication using classical techniques. For instance, the exchanged key could be used for symmetric cryptography. The security of quantum key distribution can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper, something not possible with classical key distribution. This is usually described as "unconditional security", although there are some minimal assumptions required, including that the laws of quantum mechanics apply and that Alice and Bob are able to authenticate each other, i.e. Eve should not be able to impersonate Alice or Bob as otherwise a meet-in-the-middle attack would be possible. While quantum key distribution is seemingly secure, its applications face the

challenge of practicality. This is due to transmission distance and key generation rate limitations. Ongoing studies and growing technology has allowed further advancements in such limitations. Quantum computers may become a technological reality; it is therefore important to study cryptographic schemes used against adversaries with access to a quantum computer. The study of such schemes is often referred to as post-quantum cryptography. The need for post-quantum cryptography arises from the fact that many popular encryption and signature schemes (schemes based on ECC and RSA) can be broken using Shor's algorithm for factoring and computing discrete logarithms on a quantum computer. Examples for schemes that are, as of today's knowledge, secure against quantum adversaries are McEliece and lattice-based schemes, as well as most symmetric-key algorithms.

Quantum Information Science

Quantum information science is an area of study based on the idea that information science depends on quantum effects in physics. It includes theoretical issues in computational models as well as more experimental topics in quantum physics including what can and cannot be done with quantum information. The term quantum information theory is sometimes used, but it fails to encompass experimental research in the area and can be confused with a subfield of quantum information science that studies the processing of quantum information. Subfields include: Quantum computing with studies of how and whether a quantum computer can be built and the algorithms that

harness its power, Quantum error correction, Quantum information theory, Quantum complexity theory and especially Quantum cryptography and its generalization, quantum communication.

Quantum Logic Gate

In quantum computing and specifically the quantum circuit model of computation, a quantum logic gate (or simply quantum gate) is a basic quantum circuit operating on a small number of qubits. They are the building blocks of quantum circuits, like classical logic gates are for conventional digital circuits. Unlike many classical logic gates, quantum logic gates are reversible. However, it is possible to perform classical computing using only reversible gates. For example, the reversible Toffoli gate can implement all Boolean functions, often at the cost of having to use ancilla bits. The Toffoli gate has a direct quantum equivalent, showing that quantum circuits can perform all operations performed by classical circuits. Quantum logic gates are represented by unitary matrices. The number of qubits in the input and output of the gate must be equal.

Rainbow Table

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a password (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. It is a practical

example of a space–time tradeoff, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple lookup table with one entry per hash. Use of a key derivation function that employs a salt makes this attack infeasible.

Random

Randomness is the lack of pattern or predictability in events. A random sequence of events, symbols or steps has no order and does not follow an intelligible pattern or combination. Individual random events are by definition unpredictable.

Random Number Generation

A random number generator (RNG) is a device that generates a sequence of numbers or symbols that cannot be reasonably predicted better than by a random chance. Random number generators can be true hardware random-number generators (HRNG), which generate genuinely random numbers, or pseudo-random number generators (PRNG) which generate numbers which look random, but are actually deterministic, and can be reproduced if the state of the PRNG is known. Various applications of randomness have led to the development of several different methods for generating random data, of which some have existed since ancient times, among whose ranks are well-known "classic" examples, including the rolling of dice, coin flipping, the shuffling of playing cards, the use of

yarrow stalks (for divination) in the I Ching, as well as countless other techniques. Because of the mechanical nature of these techniques, generating large numbers of sufficiently random numbers (important in statistics) required a lot of work and/or time. Thus, results would sometimes be collected and distributed as random number tables. Several computational methods for pseudo-random number generation exist. All fall short of the goal of true randomness, although they may meet, with varying success, some of the statistical tests for randomness intended to measure how unpredictable their results are (that is, to what degree their patterns are discernible). This generally makes them unusable for applications such as cryptography. However, carefully designed cryptographically secure pseudo-random number generators (CSPRNG) also exist, with special features specifically designed for use in cryptography. A cryptographically secure pseudo-random number generator (CSPRNG) or cryptographic pseudo-random number generator (CPRNG) is a pseudo-random number generator (PRNG) with properties that make it suitable for use in cryptography. Most cryptographic applications require random numbers, for example: key generation, nonces, salts in certain signature schemes, including ECDSA, RSASSA-PSS. The "quality" of the randomness required for these applications varies. For example, creating a nonce in some protocols needs only uniqueness. On the other hand, generation of a master key requires a higher quality, such as more entropy. And in the case of one-time pads, the information-theoretic guarantee of perfect secrecy only holds if the key material comes from a true random source

with high entropy, and thus any kind of pseudo-random number generator is insufficient. Ideally, the generation of random numbers in CSPRNGs uses entropy obtained from a high-quality source, generally the operating system's randomness API. However, unexpected correlations have been found in several such ostensibly independent processes. From an information-theoretic point of view, the amount of randomness, the entropy that can be generated, is equal to the entropy provided by the system. But sometimes, in practical situations, more random numbers are needed than there is entropy available. Also, the processes to extract randomness from a running system are slow in actual practice. In such instances, a CSPRNG can sometimes be used. A CSPRNG can "stretch" the available entropy over more bits. Since much cryptography depends on a cryptographically secure random number generator for key and cryptographic nonce generation, if a random number generator can be made predictable, it can be used as backdoor by an attacker to break the encryption. The NSA is reported to have inserted a backdoor into the NIST certified cryptographically secure pseudorandom number generator Dual_EC_DRBG. If for example an SSL connection is created using this random number generator, then it would allow NSA to determine the state of the random number generator, and thereby eventually be able to read all data sent over the SSL connection. Even though it was apparent that Dual_EC_DRBG was a very poor and possibly backdoored pseudorandom number generator long before the NSA backdoor was confirmed in 2013, it had seen significant usage in practice until 2013, for example by the prominent security company RSA Security. There have

subsequently been accusations that RSA Security knowingly inserted a NSA backdoor into its products, possibly as part of the Bullrun program. RSA has denied knowingly inserting a backdoor into its products.

Raspberry Pi

The Raspberry Pi is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi Foundation to promote teaching of basic computer science in schools and in developing countries. The original model became far more popular than anticipated. A Raspberry Pi can serve as a Chat Server for encrypted communication.



Figure 52: Raspberry Pi 3 B+ single-board computer as a chat server for encrypted communications [SA2]

Remote Control Systems Spyware

HackingTeam is a Milan-based information technology company that sells offensive intrusion and surveillance capabilities to governments, law enforcement agencies and

corporations. Its "Remote Control Systems" enable governments and corporations to monitor the communications of internet users, decipher their encrypted files and emails, record Skype and other Voice over IP communications, and remotely activate microphones and camera on target computers. The company has been criticized for providing these capabilities to governments with poor human rights records, HackingTeam employs around 40 people in its Italian office, and has subsidiary branches in Annapolis, Washington, D.C., and Singapore. Its products are in use in dozens of countries across six continents. This hidden mobile application grabs entered text as plaintext before it is encrypted and sent. That's why "Going the Extra Mile" is important with typing on a device, that has never been connected to the Internet for updates, and sends out the encrypted packet e.g. over a Bluetooth connection to another Internet connected device.

REPLEO

With a REPLEO the own public key is encrypted with the already received public key of a friend, so that the own public key can be transferred to the friend in a protected way.

Replay Attack

A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who

intercepts the data and re-transmits it, possibly as part of a masquerade attack by IP packet substitution. This is one of the lower tier versions of a "Man-in-the-middle attack". Another way of describing such an attack is: an attack on a security protocol using replay of messages from a different context into the intended (or original and expected) context, thereby fooling the honest participant(s) into thinking they have successfully completed the protocol run.

Requirement

Requirement is a need or expectation that is stated, generally implied or obligatory; Note: "Generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied. A specified requirement is one that is stated, for example in documented information.

RetroShare

RetroShare is a free and open-source peer-to-peer communication and file sharing app based on a friend-to-friend network built on GNU Privacy Guard (GPG). Optionally, peers may communicate certificates and IP addresses from and to their friends. That means, public peers have been replaced in this (sharing) network by trusted friends connected over a public encryption key. It is - in a complementary view - an old-fashioned way to connect to a friend, as in regard to accounts: they are not

tied to the public key of a friend. Instead an account would use cryptographic credentials.

Review

A review is an activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

Rewind

Rewind describes a function within the encrypted StarBeam-File-Transfer. With this the Send-out of a file is started for a second time. It is comparable with a new play from start of a music file. In case the file has not been completely transferred, the transmission can be started new or even scheduled for a later point of time. In case only some missing block of the file should be transferred again to the receiver, the further tool StarBeam-Analyzer is able to generate a Magnet-URI-Link, which the receiver can send to the sender, so that is will send out only the missing encrypted blocks again.

Rosetta-CryptoPad

The Rosetta-CryptoPad is part of the Spot-On encryption suite and uses an own Key for the encryption – as also an own key exists for e-mail, Chat, URLs or POPTASTIC within that suite. With the Rosetta-CryptoPad a text can be converted into cipher text. It is used, to encrypt own texts before sending the text out to the internet or before the

user posts it somewhere into the Web. Similar to the File-Encryption-Tool for Files, Rosetta also converts plaintext into ciphertext. Then the text can be transferred – either over one again secured and encrypted channel or even unencrypted as Chat or E-mail. Further messages can be posted to an Internet-Board or a Paste-Bin-Service as ciphertext. The open source tool is based on asymmetric encryption. The name derives from the Rosetta Stone.



Figure 53: Rosetta Stone [PD]

Patrons at the British Museum view the Rosetta Stone as it was displayed in 1985. The Rosetta Stone is a granodiorite stele, found in 1799, inscribed with three versions of a decree issued at Memphis, Egypt, in 196 BC during the Ptolemaic dynasty on behalf of King Ptolemy V. The top and middle texts are in Ancient Egyptian using hieroglyphic script and Demotic script, respectively, while the bottom is in Ancient Greek. As the decree has only minor differences between the three versions, the Rosetta Stone proved to be the key to deciphering Egyptian hieroglyphs, thereby opening a window into ancient Egyptian history.

ROT13

ROT13 ("rotate by 13 places", sometimes hyphenated ROT-13) is a simple letter substitution cipher that replaces a letter with the 13th letter after it, in the alphabet. ROT13 is a special case of the Caesar cipher which was developed in ancient Rome. Because there are 26 letters (2×13) in the basic Latin alphabet, ROT13 is its own inverse; that is, to undo ROT13, the same algorithm is applied, so the same action can be used for encoding and decoding. The algorithm provides virtually no cryptographic security, and is often cited as a canonical example of weak encryption. ROT13 is used in online forums as a means of hiding spoilers, punchlines, puzzle solutions, and offensive materials from the casual glance. ROT13 has inspired a variety of letter and word games on-line, and is frequently mentioned in newsgroup conversations.

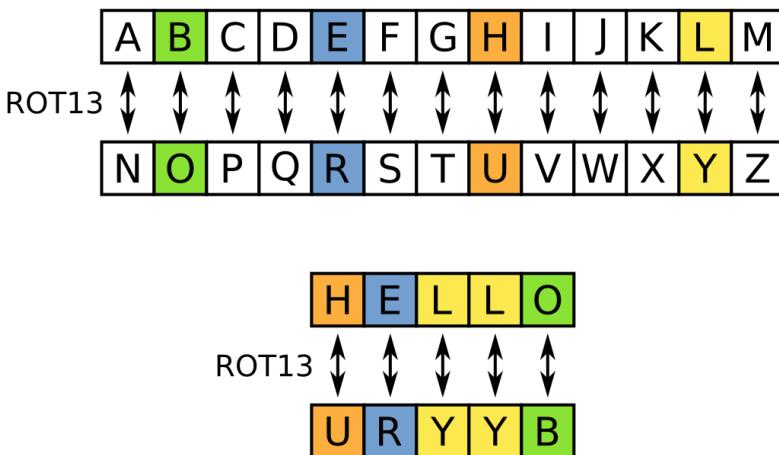


Figure 54: ROT13 replaces each letter [PD]

ROT13 replaces each letter by its partner 13 characters further along the alphabet. For example, HELLO becomes URYYB (or, conversely, URYYB becomes HELLO again).

Routing

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet. In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms. Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, gateways, firewalls, or switches. General-purpose computers also forward packets and perform routing, although they have no specially optimized hardware for the task. The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Routing tables may be specified by an administrator, learned by observing network traffic or built with the assistance of routing protocols. Routing, in a narrower sense of the term, often refers to IP routing and is contrasted with bridging. IP routing assumes that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a

single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within local area networks.

RSA

RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977/1978.

Salt, cryptographic

In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. The primary function of salts is to defend against dictionary attacks versus a list of password hashes and against pre-computed rainbow table attacks.

SCTP - Stream Control Transmission Protocol

In computer networking, the Stream Control Transmission Protocol (SCTP) is a transport-layer protocol (protocol number 132), serving in a similar role to the popular protocols Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). It provides some of the same service features of both: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP. RFC 4960 defines the protocol. RFC 3286 provides an introduction.

SECRED - Sprinkling Effect

The sprinkling effect (SE) can be understood as a watering that can feed and nourish a flower. The collected information is passed on by a node to the neighbors. Each neighbor participating in the Cryptographic Echo Discovery distributes this complementary CRED information to the other neighbors. So, every neighbor is sprinkled. S E C R E D is an acronym for the term: Sprinkling Effect via CRyptographic Echo Discovery.

Secret Streams

Secret Streams are a function within the Spot-On encryption software suite and describe a pool of keys, which are provided by a function deriving ephemeral keys created by the SMP – Socialist Millionaire Protocol – Process for authentication of two users. With this zero-

knowledge proof at both user sides keys are generated, which need not to be transferred over the internet. This invention by the Spot-On development solved the key transmission problem over the Internet.

Secure by Design

Secure by design, in software engineering, means that the software has been designed from the foundation to be secure. Malicious practices are taken for granted and care is taken to minimize impact in anticipation of security vulnerabilities, when a security vulnerability is discovered or on invalid user input. Closely related is the practice of using "good" software design as a way to increase security by reducing risk of vulnerability-opening mistakes. Generally, designs that work well do not rely on being secret. While not mandatory, proper security usually means that everyone is allowed to know and understand the design because it is secure. This has the advantage that many people are looking at the computer code, which improves the odds that any flaws will be found sooner.

Secure Channel

A secure channel is a way of transferring data that is resistant to overhearing and tampering. A confidential channel is a way of transferring data that is resistant to overhearing (i.e., reading the content), but not necessarily resistant to tampering. An authentic channel is a way of transferring data that is resistant to tampering but not necessarily resistant to overhearing. There are no perfectly

secure channels in the real world. There are, at best, only ways to make insecure channels (e.g., couriers, homing pigeons, diplomatic bags, etc.) less insecure: padlocks (between courier wrists and a briefcase), loyalty tests, security investigations, and guns for courier personnel, diplomatic immunity for diplomatic bags, and so forth. In 1976, two researchers proposed a key exchange technique (now named after them) — Diffie-Hellman key exchange (D-H). This protocol allows two parties to generate a key only known to them, under the assumption that a certain mathematical problem is computationally infeasible (i.e., very very hard) to solve, and that the two parties have access to an authentic channel. In short, that an eavesdropper — conventionally termed 'Eve', who can listen to all messages exchanged by the two parties, but who cannot modify the messages — will not learn the exchanged key. Such a key exchange was impossible with any previously known cryptographic schemes based on symmetric ciphers, because with these schemes it is necessary that the two parties exchange a secret key at some prior time, hence they require a confidential channel at that time which is just what we are attempting to build. It is important to note that most cryptographic techniques are trivially breakable if keys are not exchanged securely or, if they actually were so exchanged, if those keys become known in some other way— burglary or extortion, for instance. An actually secure channel will not be required if an insecure channel can be used to securely exchange keys, and if burglary, bribery, or threat aren't used. The eternal problem has been and of course remains—even with modern key exchange protocols—how to know when an

insecure channel worked securely (or alternatively, and perhaps more importantly, when it did not), and whether anyone has actually been bribed or threatened or simply lost a notebook (or a notebook computer) with key information in it. These are hard problems in the real world and no solutions are known—only expedients, jury rigs, and workarounds.

Secure Communication

Secure communication is when two entities are communicating and do not want a third party to listen in. For that they need to communicate in a way not susceptible to eavesdropping or interception. Secure communication includes means by which people can share information with varying degrees of certainty that third parties cannot intercept what was said. Other than spoken face-to-face communication with no possible eavesdropper, it is probably safe to say that no communication is guaranteed secure in this sense, although practical obstacles such as legislation, resources, technical issues (interception and encryption), and the sheer volume of communication serve to limit surveillance. With many communications taking place over long distance and mediated by technology, and increasing awareness of the importance of interception issues, technology and its compromise are at the heart of this debate.

Security

Security is freedom from, or resilience against, potential harm (or other unwanted coercive change) caused by others. Beneficiaries (technically referents) of security may be of persons and social groups, objects and institutions, ecosystems or any other entity or phenomenon vulnerable to unwanted change by its environment. Security mostly refers to protection from hostile forces, but it has a wide range of other senses: for example, as the absence of harm (e.g. freedom from want); as the presence of an essential good (e.g. food security); as resilience against potential damage or harm (e.g. secure foundations); as secrecy (e.g. a secure telephone line); as containment (e.g. a secure room or cell); and as a state of mind (e.g. emotional security).

Security through Obscurity

Security through obscurity (or security by obscurity) is the reliance in security engineering on the secrecy of the design or implementation as the main method of providing security for a system or component of a system. A system or component relying on obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe that if the flaws are not known, that will be sufficient to prevent a successful attack. Security experts have rejected this view as far back as 1851, and advise that obscurity should never be the only security mechanism. An early opponent of security through obscurity was the locksmith Alfred Charles Hobbs, who in 1851 demonstrated

to the public how state-of-the-art locks could be picked and who, in response to concerns that exposing security flaws in the design of locks could make them more vulnerable to criminals, said: "Rogues are very keen in their profession, and know already much more than we can teach them" (comp. Stross:2015). The principle of security through obscurity was more generally accepted in cryptographic work in the days when essentially all well-informed cryptographers were employed by national intelligence agencies, such as the National Security Agency. Now that cryptographers often work at universities, where researchers publish many or even all of their results, and publicly test others' designs, or in private industry, where results are more often controlled by patents and copyrights than by secrecy, the argument has lost some of its former popularity. An example is PGP, whose source code is publicly available to anyone, and is generally regarded as a military-grade cryptosystem.

Selectors

Selectors are fixed search keywords or criteria that are used by intelligence agencies to extract relevant information from data streams. Only encryption keeps sent plain text over the internet away from this monitoring. A selector can include metadata such as individual e-mail addresses, phone numbers, keywords, URL, geo-coordinates, MAC addresses, or the communication of a whole country. The entire message traffic from the intercepted data streams of a selector can be selectively monitored and stored. The data streams come from secret

service tapping of a deep sea cable under the Atlantic (over which a large part e.g. of the German overseas communication runs), Internet hubs, satellite communication and / or telephone and on-line offerers. The applications providing the search capabilities are called e.g. PRISM, XKeyscore, Boundless Informant, Tempora, FAIRVIEW, Genie, Bullrun and CO-TRAVELER Analytics. Because XKeyscore holds raw and unselected communications traffic, analysts can not only perform queries using "strong selectors" like e-mail addresses, but also using "soft selectors", like keywords, against the body texts of e-mail and chat messages and digital documents and spreadsheets in English, Arabic and Chinese. This is useful because "a large amount of time spent on the web is performing actions that are anonymous" and therefore those activities can't be found by just looking for e-mail addresses of a target. When content has been found, the analyst might be able to find new intelligence or a strong selector, which can then be used for starting a traditional search. According to the Spiegel, on peak days such as January 7, 2013, the NSA monitors around 60 million telephone calls e.g. in Germany from abroad: Of the 500 million monthly data records originating from Germany, which were part of the overall monitoring activities, in December 2012, 180 million entries came from XKeyscore. In May 2015, Zeit Online reports that the BND transmits far more metadata to the NSA than is known. Of the 6.6 billion metadata BND intercepts each month, up to 1.3 billion metadata are passed on to the NSA.

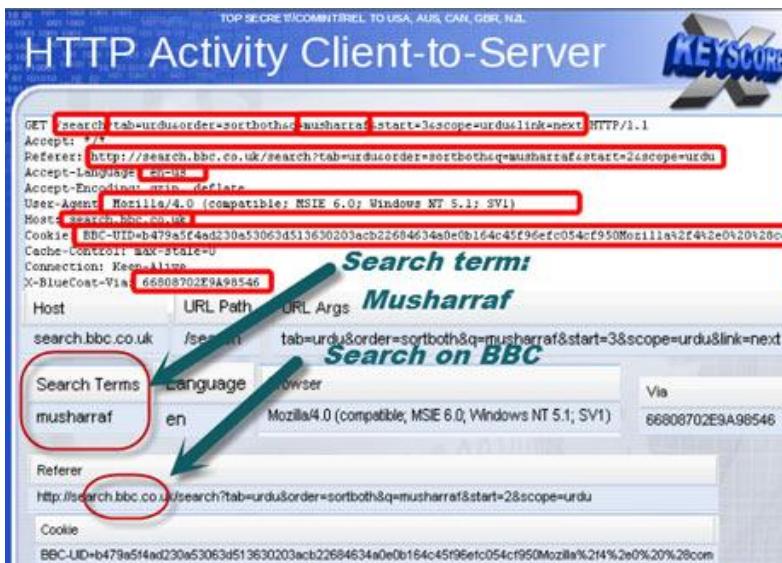


Figure 55: HTTP Activity Client-to-server: Selector chosen within the application XKeyscore

XKeyscore (XKEYSCORE or XKS) is a formerly secret computer system first used by the United States National Security Agency (NSA) for searching and analyzing global Internet data, which it collects continually. The NSA has shared XKeyscore with other intelligence agencies, including the Australian Signals Directorate, Canada's Communications Security Establishment, New Zealand's Government Communications Security Bureau, Britain's Government Communications Headquarters, Japan's Defense Intelligence Headquarters, and Germany's Bundesnachrichtendienst. In July 2013, Edward Snowden publicly revealed the program's purpose and use by the NSA in *The Sydney Morning Herald* and *O Globo* newspapers. XKeyscore consists of over 700 servers at approximately 150 sites where the NSA collects data, like "US and allied military and other facilities as well as US embassies and consulates" in many countries around the world. Among the facilities involved in the program are four bases in Australia and one in New Zealand. According to an NSA presentation from 2008, these XKeyscore servers are fed with data from several further collection systems.

Server

In computing, a server is a computer program or a device that provides functionality for other programs or devices, called "clients". This architecture is called the client–server model, and a single overall computation is distributed across multiple processes or devices. Servers can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers. A client process may run on the same device or may connect over a network to a server on a different device. Typical servers are database servers, file servers, mail servers, print servers, web servers, game servers, and application servers.

Session Management

Session Management is related to the identification of authenticated users. In computer science, in particular networking, a session is a temporary and interactive information interchange between two or more communicating devices, or between a computer and user (see login session). A session is established at a certain point in time, and then 'torn down' - brought to an end - at some later point. An established communication session may involve more than one message in each direction. A session is typically stateful, meaning that at least one of the communicating parties needs to hold current state information and save information about the session history

in order to be able to communicate, as opposed to stateless communication, where the communication consists of independent requests with responses. An established session is the basic requirement to perform a connection-oriented communication. A session also is the basic step to transmit in connectionless communication modes. However, any unidirectional transmission does not define a session.

SHA-3

SHA-3 (Secure Hash Algorithm 3) is the latest member of the Secure Hash Algorithm family of standards, released by NIST on August 5, 2015. Although part of the same series of standards, SHA-3 is internally different from the MD5-like structure of SHA-1 and SHA-2. SHA-3 is a subset of the broader cryptographic primitive family Keccak. Keccak's authors have proposed additional uses for the function, including a stream cipher, an authenticated encryption system, a "tree" hashing scheme for faster hashing on certain architectures, and AEAD ciphers Keyak and Ketje. Keccak is based on a novel approach called sponge construction. Sponge construction is based on a wide random function or random permutation and allows inputting ("absorbing" in sponge terminology) any amount of data, and outputting ("squeezing") any amount of data, while acting as a pseudorandom function with regard to all previous inputs. This leads to great flexibility.

Shared Secret

A shared secret is a piece of data, known only to the parties involved, in a secure communication. The shared secret can be a password, a passphrase, a big number or an array of randomly chosen bytes. The shared secret is either shared beforehand between the communicating parties, in which case it can also be called a pre-shared key, or it is created at the start of the communication session by using a key-agreement protocol, for instance using public-key cryptography such as Diffie-Hellman Key Exchange or using symmetric-key cryptography such as Kerberos. The shared secret can be used for authentication (for instance when logging into a remote system) using methods such as challenge-response or it can be fed to a key derivation function to produce one or more keys to use for encryption and/or MACing of messages. To make unique session and message keys the shared secret is usually combined with an initialization vector (IV). An example of this is the derived unique key per transaction method.

Shor's Algorithm

Shor's algorithm, named after mathematician Peter Shor, is a quantum algorithm (an algorithm that runs on a quantum computer) for integer factorization, formulated in 1994. Informally, it solves the following problem: Given an integer N , find its prime factors. If a quantum computer with a sufficient number of qubits could operate without succumbing to quantum noise and other quantum-decoherence phenomena, then Shor's algorithm could be

used to break public-key cryptography schemes, such as the widely-used RSA scheme. RSA is based on the assumption that factoring large integers is computationally intractable. As far as is known, this assumption is valid for classical (non-quantum) computers; no classical algorithm is known that can factor integers in polynomial time. However, Shor's algorithm shows that factoring integers is efficient on an ideal quantum computer, so it may be feasible to defeat RSA by constructing a large quantum computer. It was also a powerful motivator for the design and construction of quantum computers, and for the study of new quantum-computer algorithms. It has also facilitated research on new cryptosystems that are secure from quantum computers, collectively called post-quantum cryptography.

Side-Channel Attack

A side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited. Some side-channel attacks require technical knowledge of the internal operation of the system, although others such as differential power analysis are effective as black-box attacks. The rise of Web 2.0 applications and software-as-a-service has also significantly raised the possibility of side-channel attacks on the web, even when transmissions between a web browser and

server are encrypted (e.g., through HTTPS or WiFi encryption). Attempts to break a cryptosystem by deceiving or coercing people with legitimate access are not typically considered side-channel attacks: see social engineering and rubber-hose cryptanalysis. Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. In cryptography, rubber-hose cryptanalysis is a euphemism for the extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by coercion or torture — such as beating that person with a rubber hose, hence the name — in contrast to a mathematical or technical cryptanalytic attack.

Signal Protocol

The Signal Protocol (formerly known as the TextSecure Protocol) is a non-federated cryptographic protocol that can be used to provide end-to-end encryption for voice calls, video calls, and instant messaging conversations. The protocol was developed by Open Whisper Systems in 2013 and was first introduced in the open-source TextSecure app, which later became Signal. On 24 February 2014, Open Whisper Systems introduced TextSecure v2, which migrated to the Axolotl Ratchet. The design of the Axolotl Ratchet is based on the ephemeral key exchange that was introduced by OTR and combines it with a symmetric-key ratchet modeled after the Silent Circle Instant Messaging Protocol (SCIMP). It brought about support for asynchronous communication ("offline messages") as its

major new feature, as well as better resilience with distorted order of messages and simpler support for conversations with multiple participants. The Axolotl Ratchet was named after the critically endangered aquatic salamander Axolotl, which has extraordinary self-healing capabilities. The developers refer to the algorithm as self-healing because it automatically disables an attacker from accessing the cleartext of later messages after having compromised a session key. The third version of the protocol, TextSecure v3, made some changes to the cryptographic primitives and the wire protocol. Several closed-source applications claim to have implemented the protocol, such as WhatsApp, which is said to encrypt the conversations of "more than a billion people worldwide". Facebook Messenger also say they offer the protocol for optional Secret Conversations, as does Skype for its Private Conversations. The protocol combines the Double Ratchet algorithm, prekeys, and a triple Diffie-Hellman (3-DH) handshake, and uses Curve25519, AES-256, and HMAC-SHA256 as primitives. The Signal Protocol does not prevent a company from retaining information about when and with whom users communicate. There can therefore be differences in how messaging service providers choose to handle this information.

Simulacra

The Simulacra function is a similar function compared to the Impersonator. While Impersonator is simulating a chat of two participants with messages, Simulacra is just sending out a Fake-Message from time to time. Simulacra-Messages

contain only random characters and have not the style or goal, to imitate a process of a conversation.

SIP-Hash

SipHash is an add-rotate-xor (ARX) based family of pseudorandom functions. Although designed for use as a hash function in the computer science sense, SipHash is fundamentally different from cryptographic hash functions like SHA in that it is only suitable as a message authentication code: a keyed hash function like HMAC. That is, SHA is designed so that it is difficult for an attacker to find two messages X and Y such that $\text{SHA}(X) = \text{SHA}(Y)$, even though anyone may compute $\text{SHA}(X)$. SipHash instead guarantees that, having seen X_i and $\text{SipHash}(X_i, k)$, an attacker who does not know the key k cannot find (any information about) k or $\text{SipHash}(Y, k)$ for any message $Y \notin \{X_i\}$ which they have not seen before.

Small World Phenomenon

Small world phenomenon refers to a hypothesis, according to which every human being (social actor) is connected to the world with each other over a surprisingly short chain of acquaintance relationships. The phenomenon is often referred to as Six Degrees of Separation. Guglielmo Marconi's conjectures based on his radio work in the early 20th century, which were articulated in his 1909 Nobel Prize address, may have inspired Hungarian author Frigyes Karinthy to write a challenge to find another person to whom he could not be

connected through at most five people. This is perhaps the earliest reference to the concept of six degrees of separation, and the search for an answer to the small world problem. The small-world experiment comprised several experiments conducted by Stanley Milgram and other researchers examining the average path length for social networks of people in the United States. The research was ground-breaking in that it suggested that human society is a small-world-type network characterized by short path-lengths.



Figure 56: Path in the Small World Phenomenon [SA3]

One possible path of a message in the "Small World" experiment by Stanley Milgram.

Smoke Aliases for Key Exchange

A Smoke Alias is a unique stream of characters within Smoke Crypto Chat App. The minimum length of a Smoke Alias is eight. Similar to e-mail addresses and telephone numbers, Smoke Aliases allow simple pairing of participants. Internally, a Smoke Alias is transformed into a Smoke Identity via the SipHash algorithm. Let's consider a simple pairing scenario:

1. Participant myaddress@email.com assigns the Smoke Alias in the Public Data section of the Settings activity. Once assigned, the participant notifies other participants via e-mail or another form of communication.
2. Notified participants define myaddress@email.com within the Participants section of the Settings activity. The Smoke Alias option must be enabled.
3. Participants notify myaddress@email.com of their aliases.
4. Within new instances, the pairing is automatically initiated once the participants are online. Pairing may also be performed via the Share Keys mechanism. It is to be noted that a Smoke instance must synchronize itself with a remote server after a new Smoke Alias is assigned within Public Data. Synchronization completes in approximately 15 seconds.

Smoke Crypto Chat App

Smoke Crypto Chat is a mobile Software Echo Client Application currently for Android, which is open source, and provides with SmokeStack an easy to configure and open source server software. The user ID is not based on phone numbers and no friends list is uploaded to any

server. As it provides the secure algorithm McEliece, Smoke is regarded as worldwide the first mobile McEliece Messenger.

SmokeStack

SmokeStack is the name of the server software for encryption communication over the Smoke Crypto Chat App. It functions also as a key server and a Postbox for offline user via the Ozone function. The server is provided for the operating system Android for mobile devices.

SMTSP - Simple Mail Transfer Protocol Secured

Simple Mail Transfer Protocol Secured (SMTSP) is an Internet standard for electronic mail (email) transmission. First defined by RFC 821 in 1982, it was last updated in 2008 with the Extended SMTP additions by RFC 5321—which is the protocol in widespread use today. SMTP by default uses TCP port 25. The protocol for mail submission is the same, but uses port 587. SMTP connections secured by SSL, known as SMTSP, default to port 465.

SMP - Socialist Millionaire Protocol

In cryptography, the socialist millionaire problem is one in which two millionaires want to determine if their wealth is equal without disclosing any information about their riches to each other. It is a variant of the Millionaire's Problem

SMP - Socialist Millionaire Protocol

State Machine

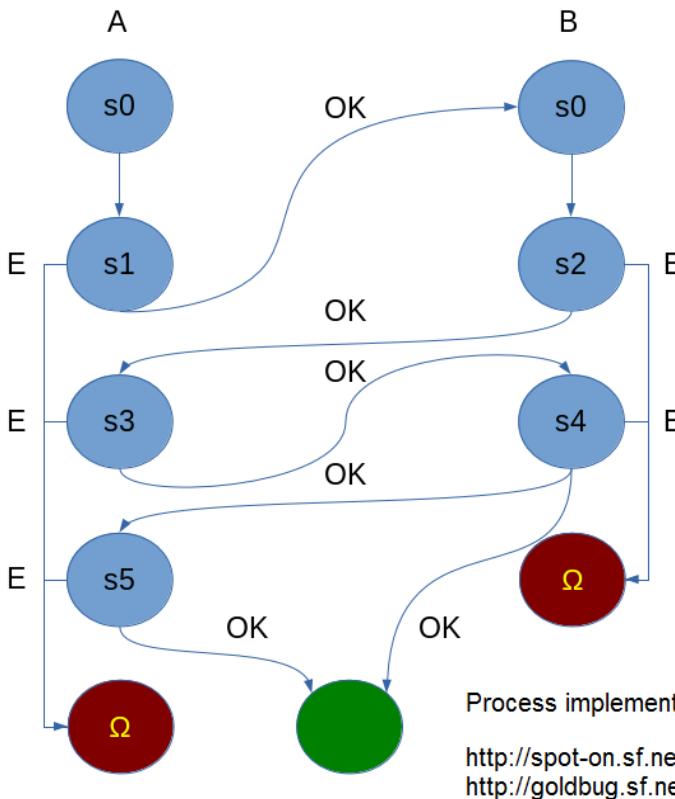


Figure 57: State machine of a socialist millionaire protocol (SMP) implementation [PD/SA4]

whereby two millionaires wish to compare their riches to determine who has the most wealth without disclosing any information about their riches to each other. It is often used as a cryptographic protocol that allows two parties to

verify the identity of the remote party through the use of a shared secret, avoiding a meet-in-the-middle attack without the inconvenience of manually comparing public key fingerprints through an outside channel. In effect, a relatively weak password/passphrase in natural language can be used.

SMP-Calling

SMP-Calling is some modus for Cryptographic Calling, which sends temporary symmetric keys for end-to-end encryption, which are derived from the Socialist Millionaire Protocol for Authentication. SMP-Calling is the basis for constantly generated temporary keys called Secret Streams.

Splitted Secret

Splitted Secrets - also called secret splitting - refer to methods for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number, of possibly different types, of shares are combined together; individual shares are of no use on their own. Secret sharing schemes are ideal for storing information that is highly sensitive and highly important. Examples include: encryption keys, missile launch codes, and numbered bank accounts. Each of these pieces of information must be kept highly confidential, as their exposure could be disastrous, however, it is also critical that they should not be lost. Traditional methods for

encryption are ill-suited for simultaneously achieving high levels of confidentiality and reliability. This is because when storing the encryption key, one must choose between keeping a single copy of the key in one location for maximum secrecy, or keeping multiple copies of the key in different locations for greater reliability. Increasing reliability of the key by storing multiple copies lowers confidentiality by creating additional attack vectors; there are more opportunities for a copy to fall into the wrong hands. Secret sharing schemes address this problem and allow arbitrarily high levels of confidentiality and reliability to be achieved. A secure secret sharing scheme distributes shares so that anyone with fewer than t shares has no more information about the secret than someone with 0 shares. Consider for example the secret sharing scheme in which the secret phrase "password" is divided into the shares

"pa____", "____ss____", "____wo__", and "_____rd".

A person with 0 shares knows only that the password consists of eight letters. He would have to guess the password from $26^8 = 208$ billion possible combinations. A person with one share, however, would have to guess only the six letters, from $26^6 = 308$ million combinations, and so on as more persons collude. Consequently, this system is not a "secure" secret sharing scheme, because a player with fewer than t secret shares is able to reduce the problem of obtaining the inner secret without first needing to obtain all of the necessary shares.

Spot-On Encryption Suite

Spot-On Encryption Suite is a secure instant chat messenger and encrypting e-mail client that also includes additional features such as group chat, file transfer, and a URL search based on an implemented URL data-base, which can be peer-to-peer connected to other nodes. Thus, the three basic functions frequently used by a regular Internet user in the Internet - communication (chat / e-mail), web search and file transfer - are represented in an encrypted environment safely and comprehensively. It can be spoken from Spot-On as of an encryption suite. It might be regarded as the most elaborated, up-to-date and diversified encryption software currently. It is based on the Echo Protocol, which sends the encrypted packets address- and target less. The three S: Speaking (by text), Searching and Sending - are now secure over the Internet within one software suite. The encryption suite is open source, written in C++ and contains as first Desktop application the algorithm McEliece.

SQLite

SQLite is a relational database management system contained in a C programming library. In contrast to many other database management systems, SQLite is not a client-server database engine. Rather, it is embedded into the end program.

StarBeam (Ultra-StarBeam)

StarBeam is the function to share a file over two Echo Clients. All packets are sent encrypted. Ultra-StarBeams transfer the file packets with sent-back receiving information, as it is within the TCP Protocol given.

StarBeam-Analyser

The StarBeam-Analyzer is a tool, to analyse a transferred file over the StarBeam-function in such a regard, if all partially blocks of the file have been received completely. The tool investigates – in case needed – the missing blocks of a file and creates a respective Magnet-URI-Link with this information. The receiver of the file can generate the Magnet and send it over to the sender of the file, who is then able to schedule a new send-out just of the missing blocks (also named as links or chunks). Over this procedure not the complete files has to be sent or replayed new to complete the original first transfer. Ultra-StarBeams have automated this process.

Steganography

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos (στεγανός), meaning "covered, concealed, or protected", and graphein (γράφειν) meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his *Steganographia*, a treatise on

cryptography and steganography, disguised as a book on magic. Generally, the hidden messages appear to be (or to be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest. Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned both with concealing the fact that a secret message is being sent and its contents. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

Stream Cipher

A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of

the keystream, to give a digit of the ciphertext stream. Since encryption of each digit is dependent on the current state of the cipher, it is also known as state cipher. In practice, a digit is typically a bit and the combining operation an exclusive-or (XOR). The pseudorandom keystream is typically generated serially from a random seed value using digital shift registers. The seed value serves as the cryptographic key for decrypting the ciphertext stream. Stream ciphers represent a different approach to symmetric encryption from block ciphers. Block ciphers operate on large blocks of digits with a fixed, unvarying transformation. This distinction is not always clear-cut: in some modes of operation, a block cipher primitive is used in such a way that it acts effectively as a stream cipher. Stream ciphers typically execute at a higher speed than block ciphers and have lower hardware complexity. However, stream ciphers can be susceptible to serious security problems if used incorrectly (called stream cipher attacks); in particular, the same starting state (seed) must never be used twice. Stream ciphers can be viewed as approximating the action of a proven unbreakable cipher, the one-time pad (OTP), sometimes known as the Vernam cipher. A one-time pad uses a keystream of completely random digits. The keystream is combined with the plaintext digits one at a time to form the ciphertext. This system was proved to be secure by Claude E. Shannon in 1949. However, the keystream must be generated completely at random with at least the same length as the plaintext and cannot be used more than once. This makes the system cumbersome to implement in many practical applications, and as a result the one-time pad has not been

widely used, except for the most critical applications. Key generation, distribution and management are critical for those applications. A stream cipher makes use of a much smaller and more convenient key such as 128 bits. Based on this key, it generates a pseudorandom keystream which can be combined with the plaintext digits in a similar fashion to the one-time pad. However, this comes at a cost. The keystream is now pseudorandom and so is not truly random. The proof of security associated with the one-time pad no longer holds. It is quite possible for a stream cipher to be completely insecure.

Super-Echo

The Echo Protocol consists of this known characteristic (if it is to be summarized), that each node tries to encrypt each message capsule: If this is successful in terms of the hash-comparison, this message is for the own reading, and will be not repacked again - and transferred further to all other connected online neighbors. As an online attacker could recognize this, when an incoming message is not sent out again to all neighbors, and thus the observer could assume, that that it is a message for the receiver at this node. With Super-Echo the message will be – even if it has been decrypted successfully for the own node – sent out again to the connected nodes for traveling on further paths. Just in regard, as this message would not have been determined for the own readings.

Surveillance

In espionage and counterintelligence, surveillance is the monitoring of behavior, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people. This can include observation from a distance by means of electronic equipment (such as closed-circuit television (CCTV) cameras) or interception of electronically transmitted information (such as Internet traffic or phone calls). It can also include simple no- or relatively low-technology methods such as human intelligence agent and postal interception. The word surveillance comes from a French phrase for "watching over" (sur means "from above" and veiller means "to watch") and is in contrast to more recent developments such as sousveillance. Surveillance is used by governments for intelligence gathering, prevention of crime, the protection of a process, person, group or object, or the investigation of crime. It is also used by criminal organisations to plan and commit crimes, such as robbery and kidnapping, by businesses to gather intelligence, and by private investigators. Surveillance can be viewed as a violation of privacy, and as such is often opposed by various civil liberties groups and activists. Liberal democracies have laws which restrict domestic government and private use of surveillance, usually limiting it to circumstances where public safety is at risk. Authoritarian government seldom have any domestic restrictions, and international espionage is common among all types of countries. The area of surveillance is increasingly a topic of academic study, including through research centers, books, and peer-reviewed academic journals.



Figure 58: Graffiti depicting state surveillance of telecommunications [CC2]

An elaborate graffiti in Columbus, Ohio, depicting state surveillance of telecommunications

In the future, intelligence services might use the internet of things for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.

Surveillance, global

Global surveillance refers to the practice of globalized mass surveillance on entire populations across national borders. Although its existence was first revealed in the 1970s and led legislators to attempt to curb domestic spying by the National Security Agency (NSA), it did not receive sustained public attention until the existence of ECHELON was revealed in the 1980s and confirmed in the 1990s. In 2013 it gained substantial worldwide media attention due to the global surveillance disclosure by Edward Snowden: Ongoing news reports in the international media have revealed operational details about the United States National Security Agency (NSA) and its international partners' global surveillance of both foreign nationals and U.S. citizens. The reports mostly emanate from a cache of top secret documents leaked by ex-NSA contractor Edward Snowden, which he obtained whilst working for Booz Allen Hamilton, one of the largest contractors for defense and intelligence in the United States. In addition to a trove of U.S. federal documents, Snowden's cache reportedly contains thousands of Australian, British and Canadian intelligence files that he had accessed via the exclusive "Five Eyes" network. In June 2013, the first of Snowden's documents were published simultaneously by The Washington Post and The Guardian, attracting considerable public attention.

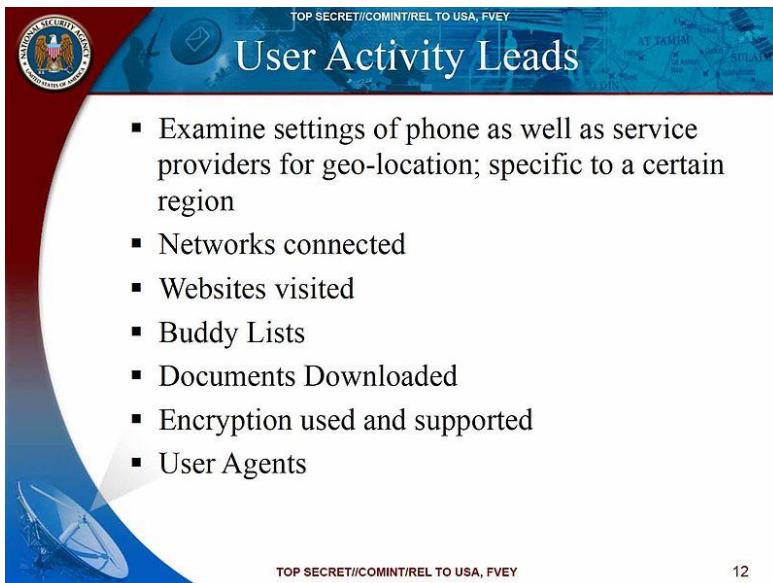


Figure 59: NSA document about surveillance on smartphones [PD]

On January 27, 2014, *The New York Times* (Risen/Poitras) released an internal NSA document from a 2010 meeting that details the extent of the agency's surveillance on smartphones. Data collected include phone settings, network connections, Web browsing history, buddy lists, downloaded documents, encryption usage, and user agents. Notice the following line of text at the bottom – "TOP SECRET//COMINT//REL TO USA, FVEY" – which is used to indicate that this top secret document is related to communications intelligence (COMINT), and can be accessed by the US and its Five Eyes (FVEY) partners in Australia, Britain, Canada, and New Zealand.

The disclosure continued throughout 2013, and a small portion of the estimated full cache of documents was later published by other media outlets worldwide. These media reports have shed light on the implications of several secret treaties signed by members of the UKUSA community in their efforts to implement global surveillance. About many

programs with different goals for data collection have been reported: PRISM, XKeyscore, Tempora, Bullrun, MUSCULAR, Project 6, Stateroom, Lustre.

The NSA was also getting data directly from telecommunications companies codenamed Artifice, Lithium, Serenade, SteelKnight, and X. The real identities of the companies behind these codenames were not included in the Snowden document dump because they were protected as Exceptionally Controlled Information which prevents wide circulation even to those who otherwise have the necessary security clearance. On June 14, 2013, United States prosecutors charged Edward Snowden with espionage and theft of government property. In late July 2013, he was granted a one-year temporary asylum by the Russian government, contributing to a deterioration of Russia–United States relations.

Symmetric Calling

Symmetric Calling is some modus for Cryptographic Calling, which sends temporary symmetric keys for end-to-end encryption. It refers to send one symmetric key (pair) through one secured channel.

Symmetric Encryption

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a

shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption , in comparison to public-key encryption (asymmetric encryption).

Symmetric Key

These keys are used with symmetric key algorithms to apply confidentiality protection to information.

TCP - Transmission Control Protocol

The Transmission Control Protocol (TCP) is a core protocol of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that emphasizes reduced latency over reliability.

The Ali Baba Cave

There is a well-known story presenting the fundamental ideas of zero-knowledge proofs, first published by Jean-Jacques Quisquater and others in their paper "How to Explain Zero-Knowledge Protocols to Your Children". It is common practice to label the two parties in a zero-knowledge proof as Peggy (the prover of the statement)

and Victor (the verifier of the statement). In this story of the Ali Baba cave, Peggy has uncovered the secret word used to open a magic door in a cave. The cave is shaped like a ring, with the entrance on one side and the magic door blocking the opposite side. Victor wants to know whether Peggy knows the secret word; but Peggy, being a very private person, does not want to reveal her knowledge (the secret word) to Victor or to reveal the fact of her knowledge to the world in general. They label the left and right paths from the entrance A and B. First, Victor waits outside the cave as Peggy goes in. Peggy takes either path A or B; Victor is not allowed to see which path she takes. Then, Victor enters the cave and shouts the name of the path he wants her to use to return, either A or B, chosen at random. Providing she really does know the magic word, this is easy: she opens the door, if necessary, and returns along the desired path. However, suppose she did not know the word. Then, she would only be able to return by the named path if Victor were to give the name of the same path by which she had entered. Since Victor would choose A or B at random, she would have a 50% chance of guessing correctly. If they were to repeat this trick many times, say 20 times in a row, her chance of successfully anticipating all of Victor's requests would become vanishingly small (about one in a million). Thus, if Peggy repeatedly appears at the exit Victor names, he can conclude that it is very probable—astronomically probable—that Peggy does in fact know the secret word. One side note with respect to third-party observers: even if Victor is wearing a hidden camera that records the whole transaction, the only thing the camera will record is in one case Victor shouting "A!"

and Peggy appearing at A or in the other case Victor shouting "B!" and Peggy appearing at B. A recording of this type would be trivial for any two people to fake (requiring only that Peggy and Victor agree beforehand on the sequence of A's and B's that Victor will shout). Such a recording will certainly never be convincing to anyone but the original participants. In fact, even a person who was present as an observer at the original experiment would be unconvinced, since Victor and Peggy might have orchestrated the whole "experiment" from start to finish. Further notice that if Victor chooses his A's and B's by flipping a coin on-camera, this protocol loses its zero-knowledge property; the on-camera coin flip would probably be convincing to any person watching the recording later. Thus, although this does not reveal the secret word to Victor, it does make it possible for Victor to convince the world in general that Peggy has that knowledge—counter to Peggy's stated wishes. However, digital cryptography generally "flips coins" by relying on a pseudo-random number generator, which is akin to a coin with a fixed pattern of heads and tails known only to the coin's owner. If Victor's coin behaved this way, then again it would be possible for Victor and Peggy to have faked the "experiment", so using a pseudo-random number generator would not reveal Peggy's knowledge to the world in the same way using a flipped coin would. Notice that Peggy could prove to Victor that she knows the magic word, without revealing it to him, in a single trial. If both Victor and Peggy go together to the mouth of the cave, Victor can watch Peggy go in through A and come out through B. This would prove with certainty that Peggy

knows the magic word, without revealing the magic word to Victor. However, such a proof could be observed by a third party, or recorded by Victor and such a proof would be convincing to anybody. In other words, Peggy could not refute such proof by claiming she colluded with Victor, and she is therefore no longer in control of who is aware of her knowledge.

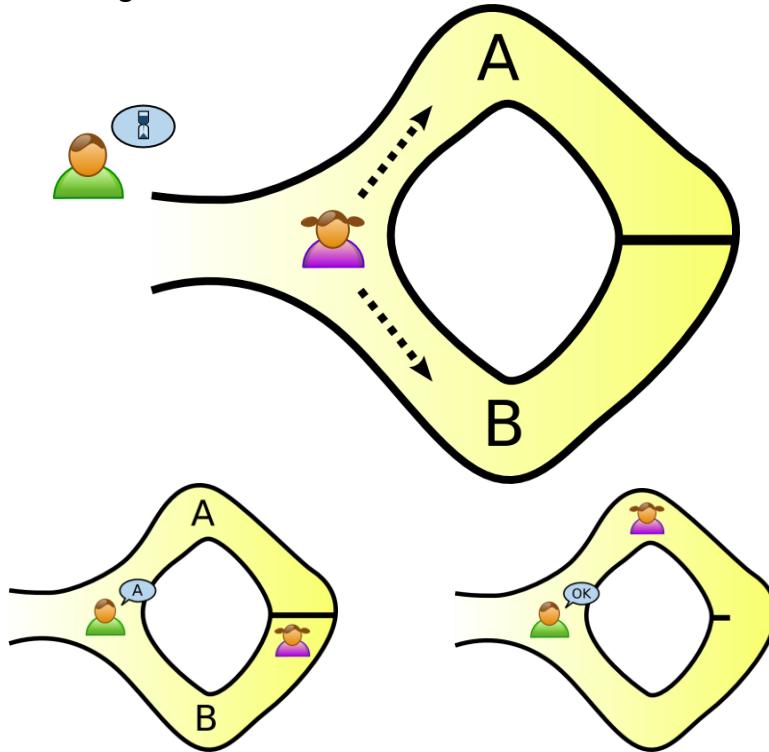


Figure 60: Peggy and Victor in the Ali Baba Cave [CC2.5]

- (A) Peggy randomly takes either path A or B, while Victor waits outside.
- (B) Victor chooses an exit path.
- (C) Peggy reliably appears at the exit Victor names.

The Bombe

The bombe is an electro-mechanical device used by Polish and British cryptologists to help decipher German Enigma-machine-encrypted secret messages during World War II. The US Navy and US Army later produced their own machines to the same functional specification, albeit engineered differently both from each other and from Polish and British Bombes. The British bombe was a development from a device that had been designed in Poland at the Biuro Szyfrów (Cipher Bureau) by cryptologist Marian Rejewski, known as the "bomba" (Polish: bomba kryptologiczna) who had been breaking German Enigma messages for the previous seven years using it and earlier machines. The initial design of the British bombe was produced in 1939 at the UK Government Code and Cypher School (GC&CS) at Bletchley Park by Alan Turing, with an important refinement devised in 1940 by Gordon Welchman. The engineering design and construction was the work of Harold Keen of the British Tabulating Machine Company. The bombe was designed to discover some of the daily settings of the Enigma machines on the various German military networks: specifically, the set of rotors in use and their positions in the machine; the rotor core start positions for the message—the message key—and one of the wirings of the plugboard.

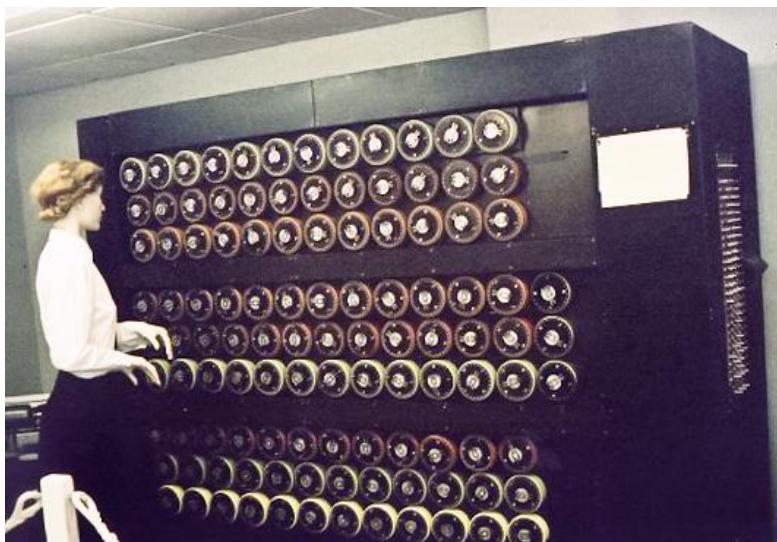


Figure 61: A wartime picture of a Bletchley Park Bombe [SA3]

The Bombe replicated the action of several Enigma machines wired together. Each of the rapidly rotating drums, pictured above in a Bletchley Park museum mockup, simulated the action of an Enigma rotor.

ThreeFish

Threefish is a symmetric-key tweakable block cipher designed as part of the Skein hash function, an entry in the NIST hash function competition. Threefish uses no S-boxes or other table lookups in order to avoid cache timing attacks; its nonlinearity comes from alternating additions with exclusive ORs. In that respect, it is similar to Salsa20, TEA, and the SHA-3 candidates CubeHash and BLAKE.

Timing

Timing is related to the race conditions, locking, or order of operations.

TLS - Transport Layer Security

Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols find widespread use in applications such as web browsing, email, instant messaging, and voice over IP (VoIP). Websites can use TLS to secure all communications between their servers and web browsers. The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. When secured by TLS, connections between a client (e.g., a web browser) and a server (e.g., wikipedia.org) should have one or more of the following three properties: (1) The connection is private (or secure) because symmetric cryptography is used to encrypt the data transmitted. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret that was negotiated at the start of the session (see § TLS handshake). The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted (see § Algorithm below). The negotiation of a shared secret is both secure (the negotiated secret is unavailable to eavesdroppers and cannot be obtained,

even by an attacker who places themselves in the middle of the connection) and reliable (no attacker can modify the communications during the negotiation without being detected). (2) The identity of the communicating parties can be authenticated using public-key cryptography. This authentication can be made optional, but is generally required for at least one of the parties (typically the server). (3) The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission. In addition to the properties above, careful configuration of TLS can provide additional privacy-related properties such as forward secrecy, ensuring that any future disclosure of encryption keys cannot be used to decrypt any TLS communications recorded in the past. TLS 1.3 spec (RFC 8446) was published in August 10, 2018. See additional Datagram Transport Layer Security (DTLS).

Token

A security token is a physical device used to gain access to an electronically restricted resource. The token is used in addition to or in place of a password. It acts like an electronic key to access something. Examples include a wireless keycard opening a locked door, or in the case of a customer trying to access their bank account online, the use of a bank-provided token can prove that the customer is who they claim to be. Some tokens may store cryptographic keys, such as a digital signature, or biometric data, such as fingerprint details. Some may also store

passwords. Tokenization, when applied to data security, is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value. The token is a reference (i.e. identifier) that maps back to the sensitive data through a tokenization system. The mapping from original data to a token uses methods which render tokens infeasible to reverse in the absence of the tokenization system, for example using tokens created from random numbers. The tokenization system must be secured and validated using security best practices applicable to sensitive data protection, secure storage, audit, authentication and authorization. The tokenization system provides data processing applications with the authority and interfaces to request tokens, or detokenize back to sensitive data. There are many ways that tokens can be classified however there is currently no unified classification. Tokens can be: single or multi-use, cryptographic or non-cryptographic, reversible or irreversible, authenticable or non-authenticable, and various combinations thereof. Tokenization and “classic” encryption effectively protect data if implemented properly, and an ideal security solution will use both. While similar in certain regards, tokenization and classic encryption differ in a few key aspects. Both are cryptographic data security methods and they essentially have the same function, however they do so with differing processes and have different effects on the data they are protecting. Tokenization is a non-mathematical approach that replaces sensitive data with non-sensitive substitutes without altering the type or length of data. This is an

important distinction from encryption because changes in data length and type can render information unreadable in intermediate systems such as databases. Tokenized data is secure, yet it can still be processed by legacy systems which makes tokenization more flexible than classic encryption.

Tor

Tor is free and open-source software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router". Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity of the user.

Tracking Cookie

Tracking cookies are used to track users' web browsing habits. This can also be done to some extent by using the IP address of the computer requesting the page or the referrer field of the HTTP request header, but cookies allow for greater precision. An HTTP cookie (also called web cookie, Internet cookie, browser cookie, or simply cookie) is a small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing. Cookies were designed to be a reliable mechanism for websites to remember stateful information (such as items added in the shopping cart in an online

store) or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past). They can also be used to remember arbitrary pieces of information that the user previously entered into form fields such as names, addresses, passwords, and credit card numbers. This can be demonstrated as follows: If the user requests a page of the site, but the request contains no cookie, the server presumes that this is the first page visited by the user. So, the server creates a unique identifier (typically a string of random letters and numbers) and sends it as a cookie back to the browser together with the requested page. From this point on, the cookie will automatically be sent by the browser to the server every time a new page from the site is requested. The server not only sends the page as usual but also stores the URL of the requested page, the date/time of the request, and the cookie in a log file. By analyzing this log file, it is then possible to find out which pages the user has visited, in what sequence, and for how long. Corporations exploit users' web habits by tracking cookies to collect information about buying habits. The Wall Street Journal found that America's top fifty websites installed an average of sixty-four pieces of tracking technology onto computers, resulting in a total of 3,180 tracking files. The data can then be collected and sold to bidding corporations. Other kinds of cookies perform essential functions in the modern web. Perhaps most importantly, authentication cookies are the most common method used by web servers to know whether the user is logged in or not, and which account they are logged in with. Without such a mechanism, the site would not know

whether to send a page containing sensitive information, or require the user to authenticate themselves by logging in. The security of an authentication cookie generally depends on the security of the issuing website and the user's web browser, and on whether the cookie data is encrypted. The tracking cookies, and especially third-party tracking cookies, are commonly used as ways to compile long-term records of individuals' browsing histories – a potential privacy concern that prompted European and U.S. lawmakers to take action in 2011. European law requires that all websites targeting European Union member states gain "informed consent" from users before storing non-essential cookies on their device.

Triad of CIA

The triad of confidentiality, integrity, and availability (CIA) is at the heart of information security. (The members of the classic InfoSec triad - confidentiality, integrity and availability - are interchangeably referred to in the literature as security attributes, properties, security goals, fundamental aspects, information criteria, critical information characteristics and basic building blocks.) However, debate continues about whether or not this CIA triad is sufficient to address rapidly changing technology and business requirements, with recommendations to consider expanding on the intersections between availability and confidentiality, as well as the relationship between security and privacy. Other principles such as "accountability" have sometimes been proposed; it has been pointed out that issues such as non-repudiation do

not fit well within the three core concepts. In 1992 and revised in 2002, the OECD's Guidelines for the Security of Information Systems and Networks proposed the nine generally accepted principles: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment. Building upon those, in 2004 the NIST's Engineering Principles for Information Technology Security proposed 33 principles. From each of these derived guidelines and practices. In 1998, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the Parkerian Hexad are a subject of debate amongst security professionals. In 2011, The Open Group published the information security management standard O-ISM3. This standard proposed an operational definition of the key concepts of security, with elements called "security objectives", related to access control (9), availability (3), data quality (1), compliance and technical (4). In 2009, DoD Software Protection Initiative released the Three Tenets of Cybersecurity which are System Susceptibility, Access to the Flaw, and Capability to Exploit the Flaw. Neither of these models are widely adopted.

Confidentiality: In information security, confidentiality is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes. While similar to "privacy," the two words aren't interchangeable. Rather, confidentiality is a component of privacy that implements to protect our data from

unauthorized viewers. Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals.

Integrity: In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically provide message integrity along side to confidentiality.

Availability: For any information system to serve its purpose, the information must be available when it is needed. This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down.

In the realm of information security, availability can often be viewed as one of the most important parts of a successful information security program. Ultimately end-users need to be able to perform job functions; by ensuring availability an organization is able to perform to the standards that an organization's stakeholders expect. This

can involve topics such as proxy configurations, outside web access, the ability to access shared drives and the ability to send emails. Executives oftentimes do not understand the technical side of information security and look at availability as an easy fix, but this often requires collaboration from many different organizational teams, such as network operations, development operations, incident response and policy/change management. A successful information security team involves many different key roles to mesh and align for the CIA triad to be provided effectively.

Non-repudiation: In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction. It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology.

Triple DES

Triple DES (3DES or TDES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block. While the government and industry standards abbreviate the algorithm's name as TDES (Triple DES) and TDEA (Triple Data Encryption Algorithm), RFC 1851 referred to it as 3DES from the time it first promulgated the idea, and this namesake has since come into wide use by most vendors, users, and

cryptographers. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm. In general, Triple DES with three independent keys (keying option 1) has a key length of 168 bits (three 56-bit DES keys), but due to the meet-in-the-middle attack, the effective security it provides is only 112 bits. Keying option 2 reduces the effective key size to 112 bits (because the third key is the same as the first). However, this option is susceptible to certain chosen-plaintext or known-plaintext attacks, and thus, it is designated by NIST to have only 80 bits of security. This can be considered broken, as the whole 3des keyspace can be searched thoroughly by affordable consumer hardware as of 2017. The short block size of 64 bits makes 3DES vulnerable to block collision attacks if it is used to encrypt large amounts of data with the same key. OpenSSL does not include 3DES by default since version 1.1.0 (August 2016), and considers it a "weak cipher".

Trojan Horse

The Trojan Horse is a story from the Trojan War about the subterfuge that the Greeks used to enter the independent city of Troy and win the war. In the canonical version, after a fruitless 10-year siege, the Greeks constructed a huge wooden horse, and hid a select force of men inside including Odysseus. The Greeks pretended to sail away, and

the Trojans pulled the horse into their city as a victory trophy. That night the Greek force crept out of the horse and opened the gates for the rest of the Greek army, which had sailed back under cover of night. The Greeks entered and destroyed the city of Troy, ending the war. Metaphorically, a "Trojan Horse" has come to mean any trick or stratagem that causes a target to invite a foe into a securely protected bastion or place. A malicious computer program which tricks users into willingly running it is also called a "Trojan horse" or simply a "Trojan". It is any malware which misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive wooden horse that led to the fall of the city of Troy. Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity. It can also delete a user's files or infect other devices connected to the network.

TEE - Trusted Execution Environment

Devices, which are not online connected and hence cannot send out taped plaintext. See "Going the Extra Mile".

Turing Machine

A Turing machine is a mathematical model of computation that defines an abstract machine, which manipulates symbols on a strip of tape according to a table of rules. Despite the model's simplicity, given any computer algorithm, a Turing machine capable of simulating that algorithm's logic can be constructed. The machine operates on an infinite memory tape divided into discrete "cells". The machine positions its "head" over a cell and "reads" or "scans" the symbol there. Then, as per the symbol and its present place in a "finite table" of user-specified instructions, the machine (i) writes a symbol (e.g., a digit or a letter from a finite alphabet) in the cell (some models allowing symbol erasure or no writing), then (ii) either moves the tape one cell left or right (some models allow no motion, some models move the head), then (iii) (as determined by the observed symbol and the machine's place in the table) either proceeds to a subsequent instruction or halts the computation. The Turing machine was invented in 1936 by Alan Turing. Alan Mathison Turing OBE FRS (23 June 1912 – 7 June 1954) was an English and homosexual mathematician, computer scientist, logician, cryptanalyst, philosopher and theoretical biologist. Turing was highly influential in the development of theoretical computer science, providing a formalization of the concepts of algorithm and computation with the Turing machine, which can be considered a model of a general-purpose computer. Turing is widely considered to be the father of theoretical computer science and artificial intelligence. Despite these accomplishments, he was never fully recognized in his home country during his lifetime.

Turing called his machine an "a-machine" (automatic machine). With this model, Turing was able to answer two questions in the negative:



Figure 62: Stephen Kettle's slate statue of Alan Turing at Bletchley Park [SA3]

The ACM A.M. Turing Award is an annual prize given by the Association for Computing Machinery (ACM) to an individual selected for contributions "of lasting and major technical importance to the computer field". The Turing Award is generally recognized as the highest distinction in computer science and the "Nobel Prize of computing".

(1) Does a machine exist that can determine whether any arbitrary machine on its tape is "circular" (e.g., freezes, or fails to continue its computational task); similarly, (2) does a machine exist that can determine whether any arbitrary machine on its tape ever prints a given symbol.

Thus, by providing a mathematical description of a very simple device capable of arbitrary computations, he was able to prove properties of computation in general - and in particular, the uncomputability of the Entscheidungsproblem ('decision problem').

Turtle-Hopping

Turtle was a free anonymous peer-to-peer network project being developed at the Vrije Universiteit in Amsterdam, involving professor Andrew Tanenbaum. Like other anonymous P2P software, it allows users to share files and otherwise communicate without fear of legal sanctions or censorship. Turtle's claims of anonymity are backed by several research papers. Technically, Turtle is a friend-to-friend (F2F) network. The RetroShare File Sharing application is based on a F2F network and implemented a "Turtle-Hopping" feature which was inspired by Turtle.

Twofish

Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Twofish's distinctive features are the use of pre-computed key-dependent S-boxes, and a relatively complex key schedule. One half of an n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent S-boxes). Twofish borrows some elements from other designs; for example, the pseudo-Hadamard transform (PHT) from the SAFER family of ciphers. The pseudo-Hadamard transform is a reversible transformation of a bit string that provides cryptographic diffusion. Twofish has a Feistel structure. A Feistel network is an iterated cipher with an internal function called a round function. Back in 2000, on most software platforms Twofish was slightly slower than Rijndael (the chosen algorithm for Advanced Encryption Standard) for 128-bit keys, but somewhat faster for 256-bit keys. But after Rijndael was chosen as the Advanced Encryption Standard, Twofish has become much slower than Rijndael on the CPUs that support the AES instruction set. The Twofish cipher has not been patented and the reference implementation has been placed in the public domain. As a result, the Twofish algorithm is free for anyone to use without any restrictions whatsoever. It is one of a few ciphers included in the OpenPGP standard (RFC 4880). However, Twofish has seen less widespread usage.

Two-Way-Calling

Two-Way-Calling is some modus for Cryptographic Calling, which creates temporary symmetric keys for end-to-end encryption, which are defined 50:50 by each of the end-users. In a Two-way Call the user sends an AES-256 as a passphrase for the future end-to-end encryption to the friend, and the friend also sends an own generated AES-256 to the first user in response. Now the first half of the AES of the first user and the second half of the AES of the second user are taken, respectively, and assembled into a common AES-256. It refers to the method of 2-way safety.

UDP - User Datagram Protocol

The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite. The protocol was designed by David P. Reed in 1980 and formally defined in RFC 768. UDP uses a simple connectionless transmission model with a minimum of protocol mechanism. It has no handshaking dialogues, and thus exposes the user's program to any unreliability of the underlying network protocol. There is no guarantee of delivery, ordering, or duplicate protection. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system.

URL - Uniform Resource Locator

A Uniform Resource Locator (URL), colloquially termed a web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A URL is a specific type of Uniform Resource Identifier (URI), although many people use the two terms interchangeably. URLs occur most commonly to reference web pages ([https](https://)) but are also used for file transfer (ftp), email ([mailto](mailto:)), database access (JDBC), and many other applications.

URL-Distiller

URL-Distillers are filter rules, with which the downloaded, uploaded or imported URLs will be filtered. For example, one can configure the URL-Distillers in such a way, that all URLs are loaded into the own Database, but only specific URLs from one defined Domain, e.g. Wikipedia, are uploaded. Also e.g. a university can distribute only URLs out of the own database to its connected students, which refer to the own web-domain. URLs and URIs of Magnets, ED2K-Links and Torrent-URLs are currently not supported in the own URL-Database respective filter rules. The distillers refer to Web-URLs and also to FTP and Gopher. URL-Distillers are a function within the URL-database of the applications GoldBug and Spot-On, which provide URL- & Bookmark-Sharing within an encrypted environment (for database & network).

URN - Uniform Resource Name

A Uniform Resource Name (URN) is a Uniform Resource Identifier (URI) that uses the urn scheme. URNs were originally conceived to be part of a three-part information architecture for the Internet, along with Uniform Resource Locators (URLs) and Uniform Resource Characteristics (URCs), a metadata framework. URNs were distinguished from URLs, which identify resources by specifying their locations in the context of a particular access protocol, such as HTTP or FTP. In contrast, URNs were conceived as persistent, location-independent identifiers assigned within defined namespaces, so that they are globally unique and persistent over long periods of time, even after the resource which they identify ceases to exist or becomes unavailable.

Vapor Protocol

The Vapor Protocol offers the traditional benefits of TCP within the environment of the Echo. A sent packet is confirmed to the sender and then the next packet will be sent. In the end no packets are missing at the receiver's site. Because of the Echo protocol, each sent packet is encrypted in a certain style and because of the graph theory aspect of the Echo protocol the transfer of each packet is complex and fuzzy – as it may take many routes. Some of the properties are described below. *Congestion Control:* Congestion control is included within the mechanisms of the Echo and is therefore separate of the Vapor Protocol. *Error Detection:* Error detection is provided by TCP as well as the acknowledgement mechanism. *Flow*

Control: Flow control is provided by the acknowledgement mechanism. A peer will not transmit a subsequent packet unless the previous packet's response has been received.

Reliable Transmission: Each packet includes a data bundle, an offset, and some header information. This information is packaged within an authentically-encrypted container. The offset indicates the order of the data bundle. A peer will transmit packets in an orderly fashion. Before a subsequent packet is transmitted, the previous packet's response must have been received by the transmitting peer.

Timeout-Based Re-transmission: If a peer has not received a transmitted packet's response within some time interval, it will transmit the packet again. This process will occur indefinitely or until the Vapor Protocol is terminated. See also Volatile Encryption.

Virtual Keyboard

As the new eavesdropping is to record the plaintext before the encryption process takes place (e.g. on mobile devices), the key logging might take place with the keyboard used on the mobile operating system. As this is mostly given by the supplier of the operating system (or a copying layer for closed source applications), it will in the future be essential to use a keyboard, which is given within an open source application: so, that the process from typing to encryption is not splitted into different processes by the operating system, but is in union with the process of the application. Hence e.g. the application GoldBug offers an own Virtual Keyboard with a double click at the login page. Here the entered text is immediately encrypted and not given to any

(intermediate) process of the operating system. The entering of the plaintext stays only in the process of the application. Only open source applications offer a review, if such a copy layer next to the keyboard is not given. Open Source applications with an own keyboard are considered safer than keyboards offered from the operating system or by closed source applications.



Figure 63: A Virtual Keyboard within the process of the encrypting (open source) application secures plaintext before it is encrypted [PD]

VEMI - Virtual E-Mail Institution

VEMI stands for Virtual E-Mail Institution. See Institution.

Vigenère Cipher

The Vigenère cipher is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It is a form of polyalphabetic substitution. First described in 1553, the cipher is easy to

understand and implement, but it resisted all attempts to break it for three centuries until 1863. This earned it the description le chiffre indéchiffrable (French for 'the indecipherable cipher'). Many people have tried to implement encryption schemes that are essentially Vigenère ciphers. In 1863, Friedrich Kasiski was the first to publish a general method of deciphering Vigenère ciphers. The Vigenère cipher was originally described by Giovan Battista Bellaso in his 1553 book La cifra del. Sig. Giovan Battista Bellaso, but the scheme was later misattributed to Blaise de Vigenère (1523–1596) in the 19th century and so acquired its present name (comp. Rodriguez-Clark:2017). In a Caesar cipher, each letter of the alphabet is shifted along some number of places. For example, in a Caesar cipher of shift 3, A would become D, B would become E, Y would become B and so on. The Vigenère cipher has several Caesar ciphers in sequence with different shift values. To encrypt, a table of alphabets can be used, termed a tabula recta, Vigenère square or Vigenère table. It has the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword. For example, suppose that the plaintext to be encrypted is

ATTACKATDAWN.

The person sending the message chooses a keyword and repeats it until it matches the length of the plaintext, for example, the keyword "LEMON": LEMONLEMONLE

Each row starts with a key letter. The rest of the row holds the letters A to Z (in shifted order). Although there are 26 key rows shown, a code will use only as many keys (different alphabets) as there are unique letters in the key string, here just 5 keys: {L, E, M, O, N}. For successive letters of the message, successive letters of the key string will be taken and each message letter enciphered by using its corresponding key row. The next letter of the key is chosen, and that row is gone along to find the column heading that matches the message character. The letter at the intersection of [key-row, msg-col] is the enciphered letter. For example, the first letter of the plaintext, A, is paired with L, the first letter of the key. Therefore, row L and column A of the Vigenère square are used, namely L. Similarly, for the second letter of the plaintext, the second letter of the key is used. The letter at row E and column T is X. The rest of the plaintext is enciphered in a similar fashion:

Plaintext: ATTACKATDAWN

Key: LEMONLEMONLE

Ciphertext: LXFOPVEFRNHR

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in that row and then using the column's label as the plaintext. For example, in row L (from LEMON), the ciphertext L appears in column A, which is the first plaintext letter. Next, in row E (from LEMON), the ciphertext X is located in column T. Thus T is the second plaintext letter.

Volatile Encryption

See also Fiasco Forwarding. The extremely volatile design using Fiasco keys or Fiasco Forwarding has significant advantages over other, more schematic protocol implementations. Volatile does not mean that the encryption is shaky or uncertain, but volatile encryption refers to changing and temporary keys that are volatile, fleeting and evaporating - thus not only decreasing the possibilities of decryption, but also multiplying the necessary decryption attempts per message and any decryption opportunities are reduced. This approach can also be found in the Vapor Protocol design. See also Vapor Protocol.

Web-of-Trust

A Web-of-Trust is a concept used in PGP, GnuPG, and other OpenPGP-compatible systems to establish the authenticity of the binding between a public key and its owner. Its decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such). As with computer networks, there are many independent webs of trust, and any user (through their identity certificate) can be a part of, and a link between, multiple webs. Networking applications that are build on a Web-of-Trust are: Delta Chat, Freenet, GoldBug, Retroshare, Spot-On and other.

Wide Lanes

One of the many obligations of a Spot-On-Kernel process is to receive, process, and forward data to one or more nodes. The mechanism that performs this task is similar to both a network hub and a network switch. Wide Lanes allow node operators to assign listener lane widths. Considering a basic example, a listener having a lane width of 20,000 bytes: The kernel, if necessary, will forward packets via the listener's clients if the sizes of the forwarded packets do not exceed 20,000 bytes. Optionally, clients may negotiate different lane widths with their peers. All network communications beyond the interface and the kernel must and will adhere to the configured limits.

XKeyscore (Surveillance Program)

XKeyscore (XKEYSCORE or XKS) is a formerly secret computer system first used by the United States National Security Agency (NSA) for searching and analyzing global Internet data, which it collects continually from plaintext send out to the Internet. The NSA has shared XKeyscore with other intelligence agencies, including the Australian Signals Directorate, Canada's Communications Security Establishment, New Zealand's Government Communications Security Bureau, Britain's Government Communications Headquarters, Japan's Defense Intelligence Headquarters, and Germany's Bundesnachrichtendienst. In July 2013, Edward Snowden publicly revealed the program's purpose and use by the

NSA in The Sydney Morning Herald and O Globo newspapers.

XMPP - Extensible Messaging and Presence Protocol

Extensible Messaging and Presence Protocol (XMPP) is a communication protocol for message-oriented middleware based on XML (Extensible Markup Language). It enables the near-real-time exchange of structured yet extensible data between any two or more network entities. Originally named Jabber, the protocol was developed by the homonym open-source community in 1999 for near real-time instant messaging (IM), presence information, and contact list maintenance. The early Jabber protocol, as developed in 1999 and 2000, formed the basis for XMPP as published in RFC 3920 and RFC 3921 (the primary changes during formalization by the IETF's XMPP Working Group were the addition of TLS for channel encryption and SASL for authentication). Note that RFC 3920 and RFC 3921 have been superseded by RFC 6120 and RFC 6121, published in 2011. One of the weaknesses is that it does not provide end-to-end encryption - in the sense of Cryptographic Calling - as a standard on every infrastructure.

XOR

XOR gate (sometimes EOR, or EXOR and pronounced as Exclusive OR) is a digital logic gate that gives a true (1 or HIGH) output when the number of true inputs is odd. An

XOR gate implements an exclusive or; that is, a true output results if one, and only one, of the inputs to the gate is true. If both inputs are false (0/LOW) or both are true, a false output results. XOR represents the inequality function, i.e., the output is true if the inputs are not alike otherwise the output is false. A way to remember XOR is "one or the other but not both". XOR can also be viewed as addition modulo 2. As a result, XOR gates are used to implement binary addition in computers. A half adder consists of an XOR gate and an AND gate. Other uses include subtractors, comparators, and controlled inverters. The behavior of XOR is summarized in the truth table shown below.

INPUT		OUTPUT
A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Figure 64: Behavior of XOR in the truth table [PD]

YaCy

YaCy (pronounced "ya see") is a free distributed search engine, built on principles of peer-to-peer (P2P) networks. Its core is a computer program written in Java distributed on several hundred computers, as of September 2006, so-called YaCy-peers. Each YaCy-peer independently crawls

through the Internet, analyzes and indexes found web pages, and stores indexing results in a common database (so called index) which is shared with other YaCy-peers using principles of P2P networks. It is a free search engine that everyone can use to build a search portal for their intranet and to help search the public internet clearly.

Zero-Knowledge-Proof

A zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that they know a value x , without conveying any information apart from the fact that they know the value x . The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information. If proving a statement requires that the prover possess some secret information, then the verifier will not be able to prove the statement to anyone else without possessing the secret information. The statement being proved must include the assertion that the prover has such knowledge, but not the knowledge itself. Otherwise, the statement would not be proved in zero-knowledge because it provides the verifier with additional information about the statement by the end of the protocol. Interactive zero-knowledge proofs require interaction between the individual (or computer system) proving their knowledge and the individual validating the proof.

Possible questions for discussion in didactic contexts:

The following questions and research fields can be discussed and addressed in didactic contexts (e.g. through the formation of groups with more than two or three people per group). Each entry in this book might have own questions. These examples are only an initial start for further needed research and development:

1. Compare different open source server software for encrypted communications. Which server software is known to you and which has already been tested?
2. Work out a content Agenda for a Crypto-Party with the integration of the Cryptographic Cafeteria game.
3. Describe a Zero-Knowledge-Proof with a Cave example.
4. Why is Cryptographic Discovery in an encrypted environment a more suitable solution rather than a DHT? Describe advantages and disadvantages.
5. Describe and compare two modes of operation of Cryptographic Calling.
6. Why should mathematicians complement their skills with computer programming knowledge?
7. Describe cases, in which a user wants to protect or hide the public key from being public - which effects has that on PKI and an architecture based on Key-Servers?
8. Why is the Echo Protocol Beyond Cryptographic Routing?
9. Describe characteristics of a third Epoch in Cryptography.
10. Why is open source code for encryption applications important? Consider the view of users, developers, the community and commercial suppliers for Server-Software and for Client-Software development and their quality management reviews.
11. Describe Fiasco Forwarding and why it is a fiasco.

12. Why is it today a heyday of end-to-end encryption? Find current examples in newspapers, where it is discussed and compare.
13. Describe main elements of the Transformation of Cryptography.
14. Why has Machine Learning turned to the new term Environmental Learning?
15. Describe the Concept of Cryptographic Tokens. Where are they deployed?
16. Why are Customer Supplied Encryptions Keys a sovereign concept?
17. Describe the encryption layers of the Echo with considering Multi-Encryption, symmetric encryption and asymmetric encryption.
18. Why and how is AutoCrypt derived from EPKS?
19. Describe the relation of Secret Streams to the Socialist-Millionaire Protocol.
20. Which trojan horses are next to possible processes of the operating system or keyboard itself known on mobile devices?
21. Describe the start of Cryptographic Calling with the symbol of the MELODICA button!
22. Which three main areas are given for creation of Multi-Encryption?
23. Discuss Life Cycle Management for RSA: Since when is RSA considered as broken?
24. Compare the terms ephemeral keys, session keys, multicast keys and fiasco keys.
25. Which role does encryption on mobile devices play? Which tools and/or functions are given?
26. Discuss the tool of a Virtual Keyboard in regard of security of typed text.
27. Which difference exists between the Juggernaut Protocol and the J-PAKE-Protocol, where it derived from? Start with the code basis.
28. Discuss the use of the McEliece algorithm in reference to Quantum Computing.

29. Which clients have the POPTASTIC Protocol implemented? Test out two different clients with your e-mail account.
30. Discuss why keyboards on mobile devices should be in the process of the application and how typed text can be secured against taping and unnoticed send outs.
31. What's the difference between Hybrid Encryption and Multi-Encryption? Give some examples with algorithms.
32. Discuss XMPP and Encryption in regard of risks and changes: Which changes need to be made?
33. What is the difference between point-to-point and end-to-end encryption?
34. When it comes to Multi-Encryption: Discuss if first RSA and then McEliece is better than vice versa?
35. Which developments has modern Cryptography to face?
36. From the code basis, which differences in procedure and coding exist between Secret Streams and the Juggernaut Protocol.
37. What is meant with the concept of "Going the Extra Mile"? How does it relate to a trusted execution environment?
38. Matrix is a subset of the Echo, right? Why?
39. How and why is Encryption related to Human Rights?
40. What is an REPLEO and which influence had it on AutoCrypt?
41. How differentiates the Signal Protocol in Key transferring from Fiasco Keys and Juggerknot Keys?
42. What is an EPKS-Channel and which cryptographic processes are behind it?
43. How is encryption ideally integrated in teaching? Give an example of an exercise.
44. What differs Instant Perfect Forward Secrecy (IPFS) from Perfect Forward Secrecy and why is that important for Security?
45. How is Exponential Encryption related to Graph Theory and the Echo?
46. Try within a software test to transmit Juggerknot Keys.
47. If one needs to learn a programming language, which language would that be in personal preference and please describe

some basic elements, which have to be learned within that language.

48. Try to build an URL Database Community with the Software GoldBug and show EPKS-Key-Share in practice to your group.
49. Compare the Sprinkling-Effect with a DHT.
50. In which regard is Turtle Hopping over POPTASTIC different from the protocol implementation in RetroShare: Which role play mobile devices for such a protocol-comparison?
51. The core of the Echo-Protocol Concept is the Echo Match. Describe in detail, what is matched.
52. Create a protocol concept and code an application for sharing files based on the POPTASTIC Protocol including Turtle Hopping.
53. Make a presentation on the implications of the Nomenklatura in GDR.
54. Compare the easiness of the administration of different servers for encrypted chat, e.g. a Matrix Server, a XMPP Server, a SmokeStack Server, a Signal Server. Find criteria to measure how difficult administration is.
55. Tell a story in terms of the Adaptive Echo about Hansel and Gretel. Which implications has this story to graph theory and information theory?
56. Read the code of the McNoodle Library: which main functions are defined?
57. Summarize the publications about Turtle Hopping; how and why it is related to a Friend-to-Friend network?
58. Why needs the right of free speech a right for encryption for the citizens? Discuss.

Index of Figures

Figure 1: Adaptive Echo Template [PD]	63
Figure 2: AddRoundKey step within the AES creation [PD]	65
Figure 3: Flowchart of Euclid's algorithm [SA4]	67
Figure 4: How asymmetric encryption with Public Key Infrastructure (PKI) works [PD]	72
Figure 5: Eight Principles of an IT Audit of cryptographic applications [PD/SA4]	77
Figure 6: 10 Trends in Cryptographic Messaging (2016) [PD]	83
Figure 7: Symbol on the cover of biometric passports [PD]	86
Figure 8: Probability of at least two people sharing a birthday [SA3]	88
Figure 9: The Caesar cipher [PD]	98
Figure 10: Two rotating disks with a Caesar cipher [PD]	100
Figure 11: Tabula recta [PD]	103
Figure 12: Ciphertext within a Web browser transferred to a HTTP Listener [PD]	104
Figure 13: The PDCA-Cycle: Plan-Do-Check-Act [SA4]	110
Figure 14: Example of a cryptogram [CC3]	115
Figure 15: Overview of the different types of Cryptographic Calling with respective criteria by Scott Edwards [PD]	116
Figure 16: The Sprinkling Effect of SECRED within Cryptographic Discovery [PD]	118
Figure 17: Diversity approach for cryptographic DNA values [PD]	119
Figure 18: Cryptographic torrents [SA3]	121
Figure 19: A flyer for a CryptoParty [CC3]	125
Figure 20: Distributed Hash Table (DHT) [PD]	134
Figure 21: Digital Signature [PD]	137
Figure 22: Cardinals eavesdropping in the Vatican [PD]	140
Figure 23: A radome to be used by ECHELON [PD]	142
Figure 24: Graphical Scheme of three encryption layers for Multi-Encryption within the Echo-Protocol [PD]	145

Figure 25: Example for the Echo-Match (within a simplified process description)	147
Figure 26: Example of a Grid-Template to explain networking [PD].....	148
Figure 27: Edgar A. Poe [PD]	150
Figure 28: Rotors of the Enigma Machine [PD/CC1]	157
Figure 29: A three-rotor Enigma with plugboard [PD]	158
Figure 30: Authenticated encryption scheme "Encrypt Then Mac" (EtM) [PD]	163
Figure 31: Authenticated encryption scheme "Encrypt and Mac" (E&M) [PD]	163
Figure 32: Authenticated encryption scheme "Mac then Encrypt" (Mte) [PD]	163
Figure 33: Four Arms in the Era of Exponential Encryption [PD]	165
Figure 34: While Silence means Security – means Free Speech in Public (or Plain Text over the Internet) the opposite? [PD].....	177
Figure 35: Gemini as term for twins representing a symmetric passphrase [PD]	181
Figure 36: Logo/Headline „Instant Definition of Decentralized Crypto“ [PD].....	185
Figure 37: The Königsberg Bridge problem [PD]	187
Figure 38: Lattice Square grid graph & 8x8 rook's graph: graph of possible moves for a standard chess rook [PD]	188
Figure 39: A perfect hash function for the four names shown [PD]	190
Figure 40: Eleanor Roosevelt and United Nations Universal Declaration of Human Rights in Spanish text [PD]	195
Figure 41: The Library of Alexandria [PD]	201
Figure 42: Early Adopters follow the Innovators for encrypted chat over e-mail servers [PD].....	202
Figure 43: Jugglers within the Karyssa I area, Egypt: Testing the truth [PD]	213

Figure 44: Example of a Magnet-URI with cryptographic values (here for a group chat Buzz channel) [PD]	231
Figure 45: Cryptographic values for the Magnet-URI standard as they are used by some encryption applications (PD)	232
Figure 46: Albert Einstein was placed under surveillance due to his alleged ties to communism [PD]	235
Figure 47: Matryoshka dolls set in a row [CC/SA3]	239
Figure 48: Carl Friedrich Gauss: “Mathematics is the queen of the sciences—and number theory is the queen of mathematics”. [PD].....	254
Figure 49: Pigeon Principle [SA3]	267
Figure 50: Settings within an application using e-mail-Servers for Chat over the POPTASTIC Protocol [PD]	274
Figure 51: Privacy may be lessened by surveillance – in this case through CCTV [SA3]	279
Figure 52: Raspberry Pi 3 B+ single-board computer as a chat server for encrypted communications [SA2].....	292
Figure 53: Rosetta Stone [PD]	296
Figure 54: ROT13 replaces each letter [PD].....	297
Figure 55: HTTP Activity Client-to-sever: Selector chosen within the application XKeyscore.....	307
Figure 56: Path in the Small World Phenomenon [SA3]	315
Figure 57: State machine of a socialist millionaire protocol (SMP) implementation [PD/SA4]	318
Figure 58: Graffito depicting state surveillance of telecommunications [CC2].....	327
Figure 59: NSA document about surveillance on smartphones [PD].....	329
Figure 60: Peggy and Victor in the Ali Baba Cave [CC2.5]	334
Figure 61: A wartime picture of a Bletchley Park Bombe [SA3].....	336
Figure 62: Stephen Kettle's slate statue of Alan Turing at Bletchley Park [SA3].....	350

- Figure 63: A Virtual Keyboard within the process of the encrypting (open source) application secures plaintext before it is encrypted [PD] 356
Figure 64: Behavior of XOR in the truth table [PD] 362

All figures are taken from Wikipedia/Wikimedia and/or have a Public Domain [labeled with: PD] e.g. Creative Commons Attribution-Share Alike 4.0 International license [labeled with: SA4] as found under: <https://creativecommons.org/licenses/by-sa/4.0/deed.en> or for the former version [labeled with: SA3] under: <https://creativecommons.org/licenses/by-sa/3.0/deed.en>; e.g. respective for the Creative Commons Attribution 3.0 unported license [labeled with: CC3] under: <https://creativecommons.org/licenses/by/3.0/deed.en> and referring versions.

Bibliography

- Aceituno, Vicente: Open Information Security Maturity Model, URL:
<http://www.ism3.com/node/39>.
- ACM Symposium (2018): 23rd ACM Symposium on Access Control Models and Technologies: 13-15 June 2018, Indianapolis, Indiana, USA, New York, NY.
- Adams, Carlisle / Lloyd, Steve (2003): Understanding PKI: concepts, standards, and deployment considerations, Addison-Wesley Professional, pp. 11-15.
- Adams, David / Maier, Ann-Kathrin (2016): BIG SEVEN Study, open source crypto-messengers to be compared - or: Comprehensive Confidentiality Review & Audit of GoldBug, Encrypting E-Mail-Client & Secure Instant Messenger, Descriptions, tests and analysis reviews of 20 functions of the application GoldBug based on the essential fields and methods of evaluation of the 8 major international audit manuals for IT security investigations including 38 figures and 87 tables., URL: <https://sf.net/projects/goldbug/files/bigseven-crypto-audit.pdf> - English / German Language, Version 1.1, 305 pages, June.
- Aharonov, Dorit (2003): A Simple Proof that Toffoli and Hadamard are Quantum Universal.
- Ajtai, Miklós (1996): Generating Hard Instances of Lattice Problems, Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. pp. 99–108.
- Akama, Seiki (2014): Elements of Quantum Computing: History, Theories and Engineering Applications, Springer.
- Akhoondi, Masoud / Yu, Curtis / Madhyastha, Harsha V. (2012): LASTor: A Low-Latency AS-Aware Tor Client (PDF). IEEE Symposium on Security and Privacy, Oakland, USA.
- Alanazi, Hamdan. O. / et al. (2010): New Comparative Study Between DES, 3DES and AES within Nine Factors, Journal of Computing, 2 (3).
- Alkim, Erdem / Ducas, Léo / Pöppelmann, Thomas / Schwabe, Peter (2015): Post-quantum key exchange - a new hope, Cryptology ePrint Archive, Report 2015/1092.
- Allen, Grant / Owens, Mike (2010): The Definitive Guide to SQLite, Apress.
- Ambrose, Jude / et al. (2010): Power Analysis Side Channel Attacks: The Processor Design-level Context, VDM Verlag.
- Anand, M. Vijay / Jayakumar C.: Secured Routing Using Quantum Cryptography, in: Krishna, P. Venkata / Babu, M. Rajasekhara / Ariwa, Ezendu (Ed.) (2011): Global Trends in Computing and Communication Systems, Volume 269 of the series Communications in Computer and Information Science, pp. 714-725, Vellore, TN, India.
- Androultsellis-Theotokis, Stephanos / Spinellis, Diomidis (2004): A survey of peer-to-peer content distribution technologies, ACM Computing Surveys, 36(4):335–371.
- Angwin, Julia (2015): The World's Email Encryption Software Relies on One Guy, Who is Going Broke, ProPublica, February 5.

- Arbeitskreis Vorratsdatenspeicherung (AKV) / Bündnis gegen Überwachung / et al. (2014): List of Secure Instant Messengers, URL: http://wiki.vorratsdatenspeicherung.de>List_of_Secure_Instant_Messengers, Mai.
- Armknecht, Frederik / Boyd, Colin / Gjøsteen, Kristian / Jäschke, Angela / Reuter, Christian / Strand, Martin (2015): A Guide to Fully Homomorphic Encryption", URL: <https://eprint.iacr.org/2015/1192>.
- Aumasson, Jean-Philippe (2017): Serious Cryptography - A Practical Introduction to Modern Encryption.
- Aumasson, Jean-Philippe / Bernstein, Daniel J. (2012): SipHash - A fast short-input PRF, URL: <https://131002.net/siphash/siphash.pdf>.
- Awodey, Steve (2006): Isomorphisms, Category theory, Oxford University Press. p. 11.
- Ayushi (2010): A Symmetric Key Cryptographic Algorithm, International Journal of Computer Applications, 1-No 15.
- Baccam, Tanya (2010): Transparent Data Encryption: New Technologies and Best Practices for Database Encryption, Sans.org. SANS Institute.
- Balducci, Alex / Meredith, Jake (2016): Matrix Olm Cryptographic Review, www.nccgroup.trust.
- Baltimorepostexaminer (2013): Edgar Allan Poe and cryptography: Are there hidden messages in Eureka?", URL: <http://baltimorepostexaminer.com/edgar-allan-poe-and-cryptography-are-there-hidden-messages-in-eureka/2013/04/27>.
- Banerjee, Sanchari / EFYTIMES News Network (2014): 25 Best Open Source Projects Of 2014: EFYTIMES ranked GoldBug Messenger # 4 on the overall Top 25 Best Open Source Projects Of 2014, URL: <http://www.efytimes.com/e1/fullnews.asp?edid=148831>.
- Baran, Paul (1960): Reliable Digital Communications Systems Using Unreliable Network Repeater Nodes, RAND Corporation papers, document P-1995, URL: <https://www.rand.org/content/dam/rand/pubs/papers/2008/P1995.pdf>, 1960.
- Baran, Paul (1964): Digital Simulation of Hot-Potato Routing in a Broadband Distributed Communications Network, URL: <http://www.rand.org/about/history/baran.list.html>.
- Barker E. / Kelsey J. (2012): Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST SP800-90A.
- Barnes, R. / Thomson, M. / Pironi, A. / Langley, A. (2015): Deprecating Secure Sockets Layer Version 3.0.
- Beckett, B. (1988): Introduction to Cryptology, Blackwell Scientific Publications.
- Bellare, M. / Namprempre, C. / T. Okamoto (Eds.) (2000): Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm, Extended Abstract in Advances in Cryptology: Asiacrypt 2000 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, 1976:531.
- Bellare, Mihir / Canetti, Ran / Krawczyk, Hugo (1996): Keying Hash Functions for Message Authentication, CRYPTO 1996, pp. 1–15.
- Bellovin, Steven / Bush, Randy (2002): Security Through Obscurity Considered Dangerous, Internet Engineering Task Force (IETF).

- Bellovin, Steven M. (2011): Frank Miller - Inventor of the One-Time Pad, *Cryptologia*, 35 (3): 203–222.
- Bender, Edward A. / Williamson, S. Gill (2010): Lists, Decisions and Graphs - With an Introduction to Probability.
- Ben-Naim, Arieh (2007): Entropy Demystified, World Scientific.
- Bennett, C.H. / Brassard, G. / Robert, J. M. (1988): Privacy amplification by public discussion, *SIAM Journal on Computing*, 17(2):210-229.
- Bennett, Charles H. / Brassard, Giles (1984): Quantum cryptography - Public key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175: 8.
- Bennett, Charles H. / et al. (1992): Experimental quantum cryptography, *Journal of Cryptology*, 5(1):3–28.
- Bennett, Deborah J. (1998): Randomness, Harvard University Press, 1998.
- Ben-Or, Michael / et. al. (1990): Everything provable is provable in zero-knowledge; in: Goldwasser, S. (Ed.): *Advances in Cryptology—CRYPTO '88*, Lecture Notes in Computer Science, 403, Springer, pp. 37–56.
- Benzekki, K. (2017): A Verifiable Secret Sharing Approach for Secure MultiCloud Storage; in: *Ubiquitous Networking*, Casablanca: Springer.
- Bergé, Claude (1958): *Théorie des graphes et ses applications*, Paris: Dunod. English edition, Wiley 1961.
- Berlekamp, Elwyn R. (1973): Goppa Codes, *IEEE Transactions on information theory*, Vol. IT-19, No. 5.
- Berners-Lee, Tim (1994): Uniform Resource Locators (URL): A Syntax for the Expression of Access Information of Objects on the Network, World Wide Web Consortium.
- Berners-Lee, Tim / Fielding, Roy / Masinter, Larry (1998): Uniform Resource Identifiers (URI): Generic Syntax, Internet Engineering Task Force.
- Bernstein, Daniel J. / Buchmann, Johannes / Dahmen, Erik (Eds.) (2009): Post-quantum cryptography, Springer.
- Bertram, Linda A. / Dooble, Gunther van (2019): Nomenclatura: What does a modern “Encyclopedia of Cryptography and Internet Security” offer for the education, discussion and sovereignty of learning professionals? - An interdisciplinary view on the Transformation of Cryptography: Fundamental concepts of Encryption, Milestones, Mega-Trends and sustainable Change in regard to Secret Communications and its Ideas, Key-Terms, Definitions and Good Practice; in: Bertram, Linda A. / Dooble, Gunther van / et al. (2019) (Eds.): *Nomenclatura - Encyclopedia of modern Cryptography and Internet Security: From AutoCrypt and Exponential Encryption to Zero-Knowledge-Proof Keys*, Norderstedt.
- Biggs, N. / Lloyd, E. / Wilson, R. (1986): Graph Theory, 1736–1936, Oxford University Press.
- Bigo, Didier / Delmas-Marty, Mireille (2011): The State and Surveillance: Fear and Control, La Clé des Langues.
- Biham, Eli / Shamir, Adi (1996): The next Stage of Differential Fault Analysis: How to break completely unknown cryptosystems.
- Black, Michael (2013): When I first heard of GoldBug - Review of GoldBug Secure Instant Messenger, URL: <http://www.lancedoma.ru/>, 29 Oct.

- Blake, I. / Seroussi, G. / Smart, N. (Eds.) (2005): Advances in Elliptic Curve Cryptography, London Mathematical Society 317, Cambridge University Press.
- Blanchette, Jasmin / Summerfield, Mark (2006): A Brief History of Qt, C++ GUI Programming with Qt 4 (1st ed.), Prentice-Hall, pp. xv–xvii.
- Blass, Andreas / Gurevich, Yuri (2003): Algorithms: A Quest for Absolute Definitions, Bulletin of European Association for Theoretical Computer Science, 81, Includes an excellent bibliography of 56 references, 2003, URL: <https://www.microsoft.com/en-us/research/wp-content/uploads/2017/01/164.pdf>.
- Bloom, D. (1973). "A Birthday Problem", American Mathematical Monthly, 80 (10): 1141–1142.
- Bloomberg (2018): The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies, <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>.
- Blum, Manuel / Feldman, Paul / Micali, Silvio (1988): Non-Interactive Zero-Knowledge and Its Applications, Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC 1988), pp. 103–112.
- BMW / BMI / BMVI DIGITALE AGENDA (2014): Entwurf – Wir wollen Verschlüsselungs-Standort Nr. 1 auf der Welt werden, Stand: 09. Juli 2014:URL: <https://netzpolitik.org/2014/wir-praesentieren-den-entwurf-der-digitalen-agenda/>.
- Bolluyt, Jess (2016): Does WhatsApp's Encryption Really Protect you? URL: <http://www.cheatsheet.com/gear-style/does-whatsapp-s-encryption-really-protect-you.html/?a=viewall>, June 03.
- Bondy, J. A. / Murty, U. S. R. (2008): Graph Theory, Springer.
- Borevich, A. I. / Shafarevich, Igor R. (1966): Number theory - Pure and Applied Mathematics, 20, Boston, MA: Academic Press.
- Borisov, Nikita / Goldberg, Ian / Brewer, Eric (2004): Off-the-Record Communication, or, Why Not To Use PGP, Workshop on Privacy in the Electronic Society.
- Borja, Mario Cortina / Haigh, John (2007): The Birthday Problem, Significance, Royal Statistical Society, 4 (3): 124–127.
- Boudot, Fabrice / Schoenmakers, Berry / Traoré, Jacques (2001): A Fair and Efficient Solution to the Socialist Millionaires' Problem, Discrete Applied Mathematics, 111 (1), pp. 23–36.
- Brendel, Jacqueline (2019): Sichere Instant Messaging Apps; in: Datenschutz und Datensicherheit, Bd. 43, 5, pp. 276–280.
- Bryant, Antonio (2014): Encryption 197 Success Secrets - 197 Most Asked Questions on Encryption - What You Need to Know, Emereo Publishing.
- Brynjolfsson, Erik / McAfee, Andrew (2014): The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies, Norton.
- Buktu, Tim (2013): NTRU: Quantum-Resistant cryptography, Independent / not affiliated with NTRU Cryptosystems, Inc.
- Bundesamt für Sicherheit in der Informationstechnik (2017): BSI-Projekt: Entwicklung einer sicheren Kryptobibliothek: Botan, URL: <https://www.bsi.bund.de/DE/Themen/>

- Kryptografie_Kryptotechnologie/ Kryptografie/ Kryptobibliothek/kryptobibliothek_node.html.
- Cakra, Deden (2014): Review of GoldBug Instant Messenger, Blogspot, URL <http://bengkelcakra.blogspot.de/2014/12/free-download-goldbug-instant-messenger.html>, 13. December.
- Calderbank, Michael (2007): The RSA Cryptosystem: History, Algorithm, Primes.
- Callegati, Franco / Cerroni, Walter / Ramilli, Marco (2009): IEEE Xplore - Man-in-the-Middle Attack to the HTTPS Protocol, ieeexplore.ieee.org: 78–81.
- Campbell, Duncan (2015): GCHQ and Me, My Life Unmasking British Eavesdroppers, The Intercept.
- Caraway, Brett Robert (2012): Survey of File-Sharing Culture, International Journal of Communication, USC Annenberg Press.
- Celi, Sofía / Bini, Ola (2018): No evidence of communication: Off-the-Record Protocol version 4.
- Cerf, Vinton G. / Kahn, Robert E. (1974): A Protocol for Packet Network Intercommunication, IEEE Transactions on Communications, 22 (5): 637–648.
- CFRG Working Group (2010): VMAC - Message Authentication Code using Universal Hashing, CFRG Working Group.
- Chabert, Jean-Luc (1999): A History of Algorithms - From the Pebble to the Microchip, Springer, Berlin.
- Chang, Ernest J. H. (1982): Echo Algorithms: Depth Parallel Operations on General Graphs, URL: <http://ieeexplore.ieee.org/iel5/32/35929/01702961.pdf?arnumber=1702961>.
- Chapweske, Justin (2001): HTTP Extensions for a Content-Addressable Web, www-talk. W3C.
- Chartrand, Gary (1985): Introductory Graph Theory, Dover.
- Chaum David (1988): The dining cryptographers' problem: unconditional sender and recipient untraceability, Journal of Cryptology, 1 (1):65–75.
- Chaum, David (1983): Blind signatures for untraceable payments, URL: <http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment>, Advances in Cryptology Proceedings of Crypto, 82(3):199–203.
- Cheon, Jung Hee; / Kim, Andrey / Kim, Miran / Song, Yongsoo (2017): Homomorphic encryption for arithmetic of approximate numbers, in: Takagi, T./ Peyrin, T. (Eds.): Advances in Cryptology – ASIACRYPT 2017, ASIACRYPT 2017, Springer, Cham. pp. 409–437.
- Christen, Michael (2005): YaCy - Peer-to-Peer Web-Suchmaschine in Die Datenschleuder, #86, p.54-57.
- Christensen, Clayton M. / Raynor, Michael E. / McDonald, Rory (2015): What Is Disruptive Innovation?, Harvard Business Review, URL: <https://hbr.org/2015/12/what-is-disruptive-innovation>, December.
- Christensen, Clayton M. (1997): The innovator's dilemma: when new technologies cause great firms to fail, Harvard Business School Press, Boston, Massachusetts, ISBN 978-0-87584-585-2.
- Chung, Key One (2004): Goppa Codes, Department of Mathematics, Iowa State University.

- Cimpanu, Catalin (2019): SHA-1 collision attacks are now actually practical and a looming danger", URL:<https://www.zdnet.com/article/sha-1-collision-attacks-are-now-actually-practical-and-a-looming-danger/>, ZDNet.
- Clarke, I. / Miller, S.G. / Hong, T.W. / Sandberg, O. / Wiley, B. (2002): Protecting free expression online with Freenet, IEEE Internet Computing, 6(1):40–9.
- Clarke, Ian / Sandberg, Oskar / Wiley, Brandon / Hong, Theodore W. (2001): Freenet: A Distributed Anonymous Information Storage and Retrieval System, Designing Privacy Enhancing Technologies, Lecture Notes in Computer Science, pp. 46–66.
- Cohn-Gordon, Katriel / et al. (2016): A Formal Security Analysis of the Signal Messaging Protocol, Cryptology ePrint Archive, IACR).
- Comer, Douglas E. / Stevens, David L. (1993): Vol III: Client-Server Programming and Applications, Internetworking with TCP/IP, Department of Computer Sciences, Purdue University, West Lafayette, IN 479: Prentice Hall.
- Constantinos / OsArena (2014): GOLDBUG: ΜΙΑ ΣΟΥΙΤΑ ΓΙΑ CHATING ΜΕ ΠΟΛΛΑΠΛΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ, URL: <http://osarena.net/logismiko/applications/goldbug-mia-souita-gia-chating-me-pollapli-kiptografisi.html>, 25 March.
- Cordasco, Jared / Wetzel, Susanne (2007): Cryptographic vs. Trust-based Methods for MANET Routing Security, URL: www.coglib.com/~jcordasc/onsite/cordasco_cryptographic_07.pdf, STM.
- Costigan, Sean / Hennessy, Michael (2016): Cybersecurity - A Generic Reference Curriculum, NATO.
- Cox, Joseph (2016): The FBI Hacked Over 8,000 Computers In 120 Countries Based on One Warrant, URL: <https://motherboard.vice.com/read/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant>, November 22.
- Crandall, Richard / Pomerance, Carl (2001): Prime Numbers - A Computational Perspective, Springer.
- Crope, Frosanta / Sharma, Ashwani / Singh, Ajit / Pahwa, Nikhil (2011): An efficient cryptographic approach for secure policy-based routing: (TACIT Encryption Technique), Electronics Computer Technology (ICECT), 2011 3rd International Conference on (Volume:5), India.
- Crovcroft, Jon. Moreton / Pratt, Tim / Twigg, Ian (2003): Peer-to-Peer Systems and the Grid, URL: <http://www.cl.cam.ac.uk/teaching/2003/AdvSysTop/grid-p2p-paper.pdf>.
- Cupa, Basil (2013): Trojan Horse Resurrected - On the Legality of the Use of Government Spyware (Govware), LISS 2013, pp. 419–428.
- Curtis, Michael Kent (2000): Free Speech - The People's Darling Privilege: Struggles for Freedom of Expression in American History, Duke University Press.
- Czeskis, A. / et. al. (2008): Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications, 3rd Workshop on Hot Topics in Security, USENIX.
- Daemen, Joan / Rijmen, Vincent (2011): The design of Rijndael - AES - The Advanced Encryption Standard, Springer, Berlin, London.
- Danesi, Marcel (2010): Cryptograms and the Allure of Secret Codes, URL: <https://www.psychologytoday.com/blog/brain>-

- workout/201009/cryptograms-and-the-allure-secret-codes, Psychology Today.
- Danezis, George (2003): Mix-Networks with Restricted Routes; in: Dingledine, Roger (Ed.): Privacy Enhancing Technologies: Third International Workshop, PET 2003, Dresden, Germany, March 26–28, Revised Papers. Vol. 3. Springer.
- Daniel J. Bernstein (2010): Grover vs. McEliece, URL: <http://cr.yp.to/codes/grovercode-20100303.pdf>.
- David, Shaw / Lutz, Donnerhacke / Rodney, Thayer / Hal, Finney / Jon, Callas (2007): OpenPGP Message Format, tools.ietf.org.
- Davies, Donald (1999): The Bombe - A Remarkable Logic Machine, Cryptologia, 23 (2): 108–138.
- Davies, Donald Watts / Barber, Derek L. A. (1973): Communication networks for computers, Computing and Information Processing, John Wiley & Sons.
- Delfs, Hans / Knebl, Helmut (2007): Symmetric-key encryption, Introduction to cryptography: principles and applications, Springer.
- Delgado-Bonal, Alfonso / Martín-Torres, Javier (2016): Human vision is determined based on information theory, Scientific Reports, 6 (1).
- Demir, Yigit Ekim (2014): Güvenli ve Hızlı Anlık Mesajlaşma Programı: GoldBug Instant Messenger programı, bu sorunun üstesinden gelmek isteyen kullanıcılar için en iyi çözümlerden birisi haline geliyor ve en güvenli şekilde anlık mesajlar gönderebilmenize imkan tanıyor (Translated: "Goldbug Instant Messenger Application is a best solution for users, who want to use one of the most secure ways to send instant messages"), News Portal Tamindir, URL: <http://www.tamindir.com/goldbug-instant-messenger/>.
- Dennedy, Michelle Finneran / Fox, Jonathan / Finneran, Thomas R. (2014): The Privacy Engineer's Manifesto - Getting from Policy to Code to QA to Value, Berkeley.
- Dhillon, G. (2007): Principles of Information Systems Security - Text and cases, John Wiley & Sons.
- Diffie, Whitfield / Hellman, Martin (1976): New directions in cryptography, 22, IEEE transactions on Information Theory, p. 644-654.
- Diffie, Whitfield / van Oorschot, Paul C. / Wiener, Michael J. (1992): Authentication and Authenticated Key Exchanges, Designs, Codes and Cryptography, 2(2):107–125
- Dijkstra, Edsger W. (1959): A note on two problems in connexion with graphs, in: Numerische Mathematik, 1, URL: <http://www-m3.ma.tum.de/twiki/pub/MN0506/WebHome/dijkstra.pdf>, pp. 269–271.
- Dimaggio, P.J. / Powell, W.W. (1983): The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160.
- Dingledine, Roger (2002): Pre-alpha: run an onion proxy now!, or-dev (Mailing list).
- Dingledine, Roger (2009): One cell is enough to break Tor's anonymity, Tor Project. 18 February.
- Dinh, Hang / Moore, Christopher / Russell, Alexander / Rogaway, Philip (Ed.) (2011): McEliece and Niederreiter cryptosystems that resist quantum Fourier

- sampling attacks, Advances in cryptology—CRYPTO 2011, Lecture Notes in Computer Science, 6841, Heidelberg, pp. 761–779.
- Dinhof, Lucas (2015): Experimentalanalyse diverser Brute-Force-Mechanismen in Linux Kali. Passwortsicherheit und Passwortkomplexität, München.
- Dobbertin, Hans / Rijmen, Vincent / Sowa, Aleksandra (Eds.) (2005): Advanced Encryption Standard - AES - 4th international conference, AES 2004, Bonn, Germany, May 10-12, 2004: revised selected and invited papers, Springer, Berlin.
- Doctorow, Cory (2012): CryptoParty - like a Tupperware party for learning crypto, Boing Boing, URL: <https://boingboing.net/2012/10/12/cryptoparty-like-a-tupperware.html>.
- Dolev, Danny / Dwork, Cynthia / Naor, Moni (2000): Nonmalleable Cryptography, SIAM Journal on Computing 30 (2), 391–437, URL: <https://dx.doi.org/10.1137%2FS0097539795291562>.
- Dooble (2006): Dooble Web Browser, URL: <http://dooble.sourceforge.net>.
- Dougherty, Chad / et. al. (2017): Secure Design Patterns, CMU.
- Dragomir, Mircea (2016): GoldBug Instant Messenger - Softpedia Review: This is a secure P2P Instant Messenger that ensures private communication based on a multi encryption technology constituted of several security layers, URL: <http://www.softpedia.com/get/Internet/Chat/Instant-Messaging/GoldBug-Instant-Messenger.shtml>, Softpedia Review, January 31st.
- Dubickis, M. / Gaile-Sarkane, E. (2015): Perspectives on Innovation and Technology Transfer, Procedia - Social and Behavioral Sciences, 213: 965–970.
- Dworkin, Morris (2011): Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode (PDF), US National Institute of Standards and Technology (NIST), Addendum to NIST Special Pub 800-38A.
- Dworkin, Morris J. (2015): SHA-3 Standard - Permutation-Based Hash and Extendable-Output Functions, Federal Inf. Process. Stds. (NIST FIPS) – 202.
- ECRYPT-CSA (2015): Post-Snowden Cryptography, URL: <https://hyperelliptic.org/PSC/>, Brussels, December 9 & 10.
- Edison, H. / Ali, N.B. / Torkar, R. (2013): Towards innovation measurement in the software industry, Journal of Systems and Software, 86 (5): 1390–1407.
- Brillouin, Leon (1956): Science and Information Theory, Mineola, N.Y.: Dover.
- Edwards, Scott / Spot-On.sf.net Project (Eds.) (2019): Communicating like dolphins with Spot-On Encryption Suite: Democratization of Multiple & Exponential Encryption; Handbook and User Manual as practical software guide with introductions into Cryptography, Cryptographic Calling and Cryptographic Discovery, P2P Networking, Graph-Theory, NTRU, McEliece, the Echo Protocol and the Spot-On Software, ISBN 9783749435067, Norderstedt.
- EFF (2016): End-to-End Encryption, EFF Surveillance Self-Defence Guide, Electronic Frontier Foundation.
- EFF projects (2018): HTTPS Everywhere.

- ElGamal, Taher (1985): A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *IEEE Transactions on Information Theory*, 31(4):469–472.
- Elstrodt, Jürgen (2007): The Life and Work of Gustav Lejeune Dirichlet (1805–1859), URL: <https://www.uni-math.gwdg.de/tschinkel/gauss-dirichlet/elstrodt-new.pdf>, Clay Mathematics Proceedings.
- Ermoshina, Ksenia / Musiani, Francesca / Halpin, Harry (2016): End-to-End Encrypted Messaging Protocols: an Overview; in: Bagnoli, Franco / et al. (Eds.): Internet Science, INSCI 2016, Florence, Italy: Springer. pp. 244–254.
- Esslinger, Bernhard (2011): Cryptography and Mathematics, URL: <https://web.archive.org/web/20110722183013/http://www.cryptool.org/download/CrypToolScript-en.pdf>, 200 pages, part of the free open-source package CrypTool.
- Esslinger, Bernhard (2016): CrypTool - An Open-Source E-Learning Project for Cryptography and Cryptanalysis", Gesellschaft fuer Informatik, Crypto Day at SAP, This presentation delivers an overview. University of Siegen.
- European Data Protection Supervisor (2008): Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, 6 August 2008.
- Even S. / Goldreich, O. (1985): On the power of cascade ciphers, *ACM Transactions on Computer Systems*, vol. 3, pp. 108–116.
- Fadilpašić, Sead (2016): WhatsApp encryption pointless, researchers claim, URL: <http://www.itportal.com/2016/05/09/whatsapp-encryption-pointless-researchers-say/>, 2016.
- Ferguson, Niels / et al. (2010): The Skein Hash Function Family - The paper in which Threefish was introduced.
- Ferraiolo, David F. / Kuhn, D. Richard / Chandramouli, Ramaswamy (2003): Role-based access control, Artech House, Boston.
- Filecluster (2015): GoldBug Instant Messenger - Un programme très pratique et fiable, conçu pour créer un pont de communication sécurisé entre deux ou plusieurs utilisateurs, URL: <https://www.filecluster.fr/logiciel/GoldBug-Instant-Messenger-174185.html>.
- Fischlin, Marc (2005): Completely Non-malleable Schemes, Automata, Languages and Programming, Lecture Notes in Computer Science, 3580, Springer, pp. 779–790.
- Flaherty, D. (1989): Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States, Chapel Hill, U.S.: The University of North Carolina Press.
- Floyd, S. / Fall, K. (1999): Promoting the Use of End-to-End Congestion Control in the Internet (IEEE/ACM Transactions on Networking, August).
- Fouché Gaines, Helen (1939): Cryptanalysis.
- Fousoft (2017): Description of GoldBug Instant Messenger, URL: <https://www.fousoft.com/goldbug-instant-messenger.html>, March 16.
- Fridrich, Jessica / M. Goljan / D. Soukal (2004): Searching for the Stego Key, Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of

- Multimedia Contents VI. Security, Steganography, and Watermarking of Multimedia Contents VI. 5306: 70–82.
- Friedman, William F. (1993): Edgar Allan Poe, Cryptographer (1936), On Poe: The Best from American Literature. Durham, NC: Duke University Press, pp. 40–54.
- Frigg, R. / Werndl, C. (2010): Entropy – A Guide for the Perplexed"; in: Probabilities in Physics; Beisbart, C. / Hartmann, S. (Eds.) Oxford University Press, Oxford.
- Gadimov, Bahtiar (2015): Initial OMEMO commit, dev.gajim.org.
- Gaffer, Tunio (2015): Why Client-Side Encryption Is the Next Best Idea in Cloud-Based Data Security, Information Security Today, Auerbach Publications.
- Gaines, Helen F. (2014): Cryptanalysis - A Study of Ciphers and Their Solution, Courier Corporation.
- Gallagher, Kevin (2014): Fifteen Months After the NSA Revelations, Why Aren't More News Organizations Using HTTPS?, Freedom of the Press Foundation.
- Gartner, Richard (2016: Metadata - Shaping Knowledge from Antiquity to the Semantic Web, Springer.
- Garvie, Clare / Bedoya, Alvaro / Frankle, Jonathan (2016): Perpetual Line Up: Unregulated Police Face Recognition in America, Center on Privacy & Technology at Georgetown Law.
- Gasakis, Mele / Schmidt, Max (2018): Beyond Cryptographic Routing: The Echo Protocol in the new Era of Exponential Encryption (EEE) - A comprehensive essay about the Sprinkling Effect of Cryptographic Echo Discovery (SECRED) and further innovations in cryptography around the Echo Applications Smoke, SmokeStack, Spot-On, Lettera and GoldBug Crypto Chat Messenger addressing Encryption, Graph-Theory, Routing and the change from Mix-Networks like Tor or I2P to Peer-to-Peer-Flooding-Networks like the Echo respective to Friend-to-Friend Trust-Networks like they are built over the POPTASTIC protocol, ISBN 978-3-7481-5198-2, Norderstedt.
- Generation NT (2014): Sécuriser ses échanges par messagerie: Apportez encore plus de la confidentialité dans votre messagerie, URL: <https://www.generationnt.com/goldbug-messenger-securiser-echanger-communiquer-discuter-messagerie-securite-echange-communication-telecharger-telechargement-1907585.html>.
- Gentry, Craig (2009): A Fully Homomorphic Encryption Scheme, Stanford, CA, USA: Stanford University.
- Gibbons, Alan (1985): Algorithmic Graph Theory, Cambridge University Press.
- Glendon, Mary Ann (2001): A World Made New: Eleanor Roosevelt and the Universal Declaration of Human Rights, Random House of Canada Ltd..
- Godwin, Dan (2012): Passphrases only marginally more secure than passwords because of poor choices, URL: <https://arstechnica.com/information-technology/2012/03/passphrases-only-marginally-more-secure-than-passwords-because-of-poor-choices/>.
- Goldberg, Ian / Stedman, Ryan / Yoshida, Kayo (2008): A User Study of Off-the-Record Messaging, University of Waterloo, Symposium on Usable Privacy and Security (SOUPS) 2008, July 23–25, Pittsburgh, PA, USA, URL:

- http://www.cypherpunks.ca/~iang/pubs /otr_userstudy.pdf, & URL:
<https://otr.cypherpunks.ca/Protocol-v3-4.0.0.html>.
- Goldreich, Oded / Goldwasser, Shafi / Halevi, Shai (1997): Public-key cryptosystems from lattice reduction problems, in: CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, p.p. 112–131, London, UK.
- Golumbic, Martin (1980): Algorithmic Graph Theory and Perfect Graphs, Academic Press.
- Goodin, Dan (2013): Think your Skype messages get end-to-end encryption? Think again, Ars Technica. Kivinen, T. / M. Kojo (2003): RFC 3526 – More Modular Exponential (MODP) Diffie–Hellman groups for Internet Key Exchange (IKE), SSH Communications Security, May.
- Goodwins, Rupert (2000): Echelon: How it works, URL: <http://www.zdnet.com/echelon-how-it-works-3002079849/>, ZDNet.
- Gordon, Adam (2015): Official (ISC)2 Guide to the CISSP CBK - Fourth Edition, (ISC)2 Press.
- Gosling, James / et. al. (2014): The Java® Language Specification, (Java SE 8 ed.).
- Grabher, Philipp / et al. (2007): Cryptographic Side-Channels from Low-power Cache Memory; in: Galbraith, Steven D. (Ed.): Cryptography and coding: 11th IMA International Conference, Cirencester, UK.
- Greenwald, Glenn / Ackerman, Spencer (2013): How the NSA Is Still Harvesting Your Online Data – Files Show Vast Scale of Current NSA Metadata Programs, with One Stream Alone Celebrating 'One Trillion Records Processed', The Guardian.
- Grumbling, Emily / Horowitz, Mark (Eds.) (2018): Quantum Computing - Progress and Prospects, Washington, DC: National Academies Press.
- Gultsch, Daniel (2018): Federated Instant Messaging with Jabber/XMPP - FOSSASIA 2018, published 25.03.2018, Min: 8:55, outdated XMPP servers: jabber.systemausfall.org, jabber.hot-chilli.net, elaoon.de, jabber.fr, jabber.de, high-way.me, bommboo.de, mail.de; URL: https://www.youtube.com/watch?v=5pJYQG_oKks
- Halabi, Sam (2000): Internet Routing Architectures, Cisco Press.
- Hao, F. / Ryan, P. (2008): Password Authenticated Key Exchange by Juggling, Proceedings of the 16th International Workshop on Security Protocols.
- Hao, F. / Ryan, P. (2019): J-PAKE - Authenticated Key Exchange Without PKI, Springer Transactions on Computational Science XI, Special Issue on Security in Computing, Part II, Vol. 6480, pp. 192–206.
- Haque, Akhlaque (2015): Surveillance, Transparency and Democracy: Public Administration in the Information Age. University of Alabama Press, Tuscaloosa, AL.
- Harary, Frank (1969): Graph Theory, Reading, Massachusetts: Addison-Wesley.
- Hartshorn, Sarah (2015): GoldBug Messenger among 3 New Open Source Secure Communication Projects, URL: <http://blog.vuze.com/2015/05/28/3-new-open-source-secure-communication-projects/>, May 28.
- Harvey, Cynthia / Datamation (2015): 50 Noteworthy Open Source Projects – Chapter Secure Communication: GoldBug Messenger ranked on first # 1 position, URL: <http://www.datamation.com/open-source/50-noteworthy-new-open-source-projects-3.html>, posted September 19.
- Hazewinkel, Michiel (Ed.) (2001): Isomorphism, Encyclopedia of Mathematics, Springer.

- Hazewinkel, Michiel (Ed.) (2001): Turing machine; in: Encyclopedia of Mathematics, Springer.
- Hazewinkel, Michiel (Ed.) (2001/1994): Chaos, Encyclopedia of Mathematics, Springer.
- Heise (2014): GoldBug kann Schlüssel selbst encodiert versenden, URL: <http://www.heise.de/download/goldbug-1192605.html>.
- Heitz, Ryan (2016): Hello Raspberry Pi!.
- Hell, Pavol (1978): Graphs with given neighborhoods I, Problèmes combinatoires et théorie des graphes, Colloques internationaux C.N.R.S., 260, pp. 219–223.
- Henry, Jasmine (2018): What is Crypto-Agility?, Cryptomathic, URL: <https://www.cryptomathic.com/news-events/blog/what-is-crypto-agility>.
- Herrmann, Michael (2011): Auswirkung auf die Anonymität von performanzbasierter Peer-Auswahl bei Onion-Routern: Eine Fallstudie mit I2P, Masterarbeit, München, <https://gnunet.org/sites/default/files/herrmann2011mt.pdf>.
- Herstein, I. N. (1964): Topics in Algebra, Waltham: Blaisdell Publishing Company.
- Hildenbrand, Jerry (2016): Everyone is a node: How Wi-Fi Mesh Networking work, URL: <https://www.androidcentral.com/how-wifi-mesh-networks-work>.
- Hinsley, F. H. / Stripp, A. (Eds.). (1993): The Enigma Machine - Its Mechanism and Use. Codebreakers: The Inside Story of Bletchley Park.
- Hobbit (1995): New tool available: Netcat, Bugtraq mailing list.
- Hoffstein, Jeffrey / Pipher, Jill / Silverman, Joseph H. (1998): NTRU - A ring-based public key cryptosystem, Algorithmic Number Theory, Lecture Notes in Computer Science, 1423, pp. 267–288.
- Hofheinz, Dennis / Kiltz, Eike (2007): Secure Hybrid Encryption from Weakened Key Encapsulation, Advances in Cryptology, CRYPTO 2007, Springer, pp. 553–571.
- Holstein, Otto (1921): The ciphers of Porta and Vigenère: The original undecipherable code, and how to decipher it, Scientific American Monthly, 4: 332–334.
- Honan, Mat (2012): Kill the Password - Why a String of Characters Can't Protect Us Anymore, Wired.
- Honda, Osamu / Ohsaki, Hiroyuki / Imase, Makoto / Ishizuka, Mika / Murayama, Junichi (2005): Understanding TCP over TCP: effects of TCP tunneling on end-to-end throughput and latency.
- Hornstein, Ken (2000): Kerberos FAQ, v2.0, Secretary of Navy.
- Horváth, Máté / Buttyán, Levente (2019): Cryptographic Obfuscation - A Survey, Cham: Springer International Publishing.
- Houmkozlis, Christos N. / Rovithakis, George A. (2012): End-to-end adaptive congestion control in TCP/IP networks; in: Automation and control engineering series, CRC Press, Boca Raton, Fla.
- Howlader, Jaydeep / Basu, Saikat (2009): Sender-Side Public Key Deniable Encryption Scheme, Proceedings of the International Conference on Advances in Recent Technologies in Communication and Computing. IEEE.
- Howlader, Jaydeep / Nair, Vivek / Basu, Saikat (2011): Deniable Encryption in Replacement of Untappable Channel to Prevent Coercion, Proc. Advances in Networks and Communications, Communications in Computer and Information Science. 132, Springer, pp. 491–501.

- Huang, Yahsin (2019): Decentralized Public Key Infrastructure (DPKI): What is it and why does it matter?, Hacker Noon.
- Hughes, Jeff / Cybenko, George (2018): Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity, Technology Innovation Management Review, 3 (8), URL: <http://www.timreview.ca/article/712>.
- Huitema, Christian (2000): Routing in the Internet, Second Ed. Prentice-Hall.
- Informationweek (2016): Google's Cloud Lets You Bring customer-supplied encryption keys (CSEK), URL: <http://www.informationweek.com/cloud/infrastructure-as-a-service/googles-cloud-lets-you-bring-your-own-encryption-keys/d/d-id/1326482>.
- Ingham, Kenneth / Forrest, Stephanie (2002): A History and Survey of Network Firewalls, URL: <https://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf>.
- ISO/IEC 9797-1 (2011): Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, ISO/IEC.
- Jablon, David P. (1996): Strong Password-Only Authenticated Key Exchange, ACM Computer Communication Review, 26 (5):5–26.
- Jackson, Patrick Thaddeus / Neson, Daniel H. (2003): Representation is Futile?: American Anti-Collectivism and the Borg; in: Weldes, Jutta (Ed.): To Seek Out New Worlds: Science Fiction and World Politics, pp:143–167.
- Johnson, K. (2000): Internet E-mail Protocols - A Developer's Guide, Addison-Wesley Professional.
- Joint Committee on Human Rights (2007): Government response to the Committee's fourteenth report of session 2007-08, Data protection and human rights - twenty-second report of session 2007-08, report, together with formal minutes, and an appendix.
- Joos, Thomas (2014): Sicheres Messaging im Web, URL: http://www.pcwelt.de/ratgeber/Tor_I2p_Gnutella_RetroShare_Freenet_GoldBug_Spurlos_im_Web-Anonymisierungsnetzwerke-8921663.html, PCWelt Magazin, 01. Oktober.
- Jøsang, Audun (2017): A Consistent Definition of Authorization, Proceedings of the 13th International Workshop on Security and Trust Management (STM 2017).
- Joseph L. Bower, Clayton M. Christensen (1995): Disruptive Technologies, Catching the Wave, in: Harvard Business Review, ISSN 0007-6805, Bd. 69 pp. 19–45.
- Joux, Antoine (2009): Algorithmic Cryptanalysis, CRC Press.
- Kalt, Christophe (2000): Internet Relay Chat - Architecture.
- Kankowski, Peter (2008): Hash functions: An empirical comparison, URL: https://www.strchr.com/hash_functions.
- Karinthy, Frigyes (1929): Chain Links, URL: https://djjr-courses.wdfiles.com/local--files/soc180%3Akarinthy-chain-links/Karinthy-Chain-Links_1929.pdf
- Karinthy, Frigyes (1929): Láncszemek.
- Katz, Jonathan (2015): Public-key cryptography - PKC 2015: 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, Heidelberg, Springer.
- Katz, Jonathan / Lindell, Yehuda (2014): Introduction to Modern Cryptography, Chapman & Hall/CRC Cryptography and Network Security.

- Kayem, Anne V. D. M. / Akl, Selim G. / Martin, Patrick (2010): Adaptive Cryptographic Access Control, Springer US, Boston, MA.
- Kenneth H. Rosen (2010): Elementary Number Theory, Pearson Education.
- Kerckhoffs, Auguste (1883): La cryptographie militaire, Journal des sciences militaires, vol. IX, pp. 5–83, January 1883, pp. 161–191.
- Kerner, Sean Michael: NSA Bullrun, 9/11 and Why Enterprises Should Walk Before They Run, Eweek.com.
- King, D.A. (2001): The Ciphers of the Monks - A Forgotten Number-notation of the Middle Ages, Stuttgart: Steiner, p. 171.
- Kišasondi, Tonimir / Hutinski, Željko (2009): Cryptographic routing protocol for secure distribution and multiparty negotiatiated access control, URL: <http://www.ceciis.foi.hr/app/index.php/ceciis/2009/paper/download/219/209>, Varazdin, Croatia.
- Kleinberg, Jon (2000): The Small-World Phenomenon: An Algorithmic Perspective, Proceedings of the thirty-second annual ACM symposium on Theory of computing, pp. 163–70.
- Knudsen, Lars R. / Robshaw, Matthew (2011): The Block Cipher Companion, Springer.
- Knuth, Donald E. (1987): The Art of Computer Programming. Vol. 2: Seminumerical Algorithms, MA: Addison-Wesley.
- Koch, Werner (2016): OpenPGP Web Key Service draft-koch-openpgp-webkey-service-00, URL: <https://tools.ietf.org/html/draft-koch-openpgp-webkey-service-00>, May.
- Koch, Werner (2019): Announce - GnuPG 2.2.16 released, gnupg-announce (Mailing list).
- Kocher, Paul C. (1996): Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. CRYPTO, pp. 104–113.
- König, Dénes (1936): Theorie der Endlichen und Unendlichen Graphen: Kombinatorische Topologie der Streckenkomplexe, Akademische Verlagsgesellschaft, Leipzig 1936.
- Kors, Alan Charles (2008): Freedom of Speech"; in: Hamowy, Ronald (Ed.): The Encyclopedia of Libertarianism. Thousand Oaks, CA: SAGE, Cato Institute, pp. 182–85.
- Kostomárova, Elena (2015): More than just a pretty face - The secrets of the Russian matryoshka.
- Kozaczuk, Władysław / Kasparek, Christopher (Eds.) (1984): Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two, Frederick, MD: University Publications of America.
- Kreibich, Jay A. (2010): Using SQLite, O'Reilly Media.
- Kuczma, M. / Choczewski B. / Ger, R. (1990): Iterative Functional Equations, Cambridge University Press.
- Künast, Renate (2018): Algorithmen: >Ethik-by-Design< – Diskriminierung systematisch verhindern, in: (Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, Sammelband des Fraunhofer Instituts (ÖFIT), edited by: Resa Mohabbat Kar, Basanta Thapa, Peter Parycek, pp. 553–560
- Kurawar, Arwa / Koul, Ayushi / Patil, Viki Tukaram (2014): Survey of Bluetooth and Applications, International Journal of Advanced Research in Computer Engineering & Technology, 3:2832–2837.

- Lachance, Dan (2015): Cryptography Fundamentals - Describing How Cryptography Provides Confidentiality, Nashua, New Hampshire: Skillssoft Corporation.
- Lanyon, B. P. / et al. (2007): Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement, *Physical Review Letters*, 99 (25): 250505.
- L'Ecuyer, Pierre (2017): History of Uniform Random Number Generation; in: Proceedings of the 2017 Winter Simulation Conference, IEEE Press, pp. 202–230.
- Leiner, Barry M. / et.al. (2003): A Brief History of Internet.
- Lennon, Brian (2018): Passwords: Philology, Security, Authentication, Harvard University Press.
- Lenstra, Arjen K. / Verheul, Eric R. (2001): Selecting Cryptographic Key Sizes, *J. Cryptology* 14(4): 255–293.
- Levine, Yasha (2014): Almost everyone involved in developing Tor was (or is) funded by the US government - How leading Tor developers and advocates reacted after I reported their US Government ties, URL: <https://pando.com/2014/11/14/tor-smear/>, written on November 14.
- Lewis, Anthony (2007): Freedom for the Thought That We Hate: A Biography of the First Amendment, Basic Books.
- Li. J. / Dabek, F. (2006): F2F: Reliable Storage in Open Networks, in: 5th International Workshop on Peer-to-Peer Systems (IPTPS '06), Santa Barbara, CA, USA, February.
- Liang, Y. / Vincent Poor, H. / Shamai, S. (2008): Information Theoretic Security, Foundations and Trends in Communications and Information Theory, 5(4–5):355–580.
- Lim, Joo S. / et al. (2009): Exploring the Relationship between Organizational Culture and Information Security Culture, Australian Information Security Management Conference.
- Lindner, Mirko (2014): POPTASTIC: Verschlüsselter Chat über POP3 mit dem GoldBug Messenger, Pro-Linux, URL: <http://www.pro-linux.de/news/1/21822/poptastic-verschluesselter-chat ueber-pop3.html>, 9. Dezember.
- Lindsay, G. (1999): The government is reading your E-Mail. *TIME DIGITAL DAILY*, June.
- Linuxfound (2016): Open Source Development and Sustainability - A Look at the Bouncy Castle Project, Linux Foundation Collaboration Summit, URL: <http://events.linuxfoundation.org/sites/events/files/slides/BCCCollabTalkSlides.pdf>.
- Liz, Crowcroft; et al. (2005): A survey and comparison of peer-to-peer overlay network schemes, *IEEE Communications Surveys & Tutorials*, 7(2):72–93.
- Luby M. (1996): Pseudorandomness and Cryptographic Applications, Princeton Univ Press.
- Luciano, Dennis / Gordon Prichett (1987): Cryptology: From Caesar Ciphers to Public-Key Cryptosystems, *The College Mathematics Journal*, 18(1):2–17.
- Lyon, David (2007): Surveillance Studies - An Overview, Cambridge: Polity Press.
- Lyon, David (2015): Surveillance After Snowden, John Wiley & Sons.
- Macaulay, Tyson (2019): Cryptographic Agility in Practice, URL: https://uploads-ssl.webflow.com/5bd73d456f7b3f2db2bbb95/5c76a740dcc2cc4646a06805_ISG_AgilityUseCases_Whitepaper-FINAL.pdf, InfoSec Global.

- Majorgeeks (2013): GoldBug Secure Email Client & Instant Messenger, URL:http://www.majorgeeks.com/files/details/goldbug_secure_email_Client_instant_messenger.html.
- Manral, V. / Bhatia, M. / Jaeggli, J. / White, R. (2010): Issues with Existing Cryptographic Protection Methods for Routing Protocols, URL: <http://info.internet.isi.edu/in-notes/pdrrfc/fc6039.txt.pdf>.
- Marconi, Guglielmo (1909): Nobel Lecture, Wireless telegraphic communication.
- Markov, A.A. (1954): Theory of algorithms - Imprint Moscow, Academy of Sciences of the USSR.
- Marlinspike, Moxie (2013): Advanced cryptographic ratcheting, Blog, Open Whisper Systems.
- Mason, Stephen (2016): Electronic Signatures in Law, 4th edition, Institute of Advanced Legal Studies for the SAS Digital Humanities Library, School of Advanced Study, University of London.
- Stark, Scott (2005): DIGEST Authentication (4.0.4+), JBoss.
- Matejka, Petr: Model of Turtle network, in: Security in Peer-to-Peer Networks, Master Thesis. URL: <http://turtle-p2p.sourceforge.net/thesis2.pdf>.
- Matrix / Johnston, Erik (2014): Matrix - An open standard for decentralised persistent communication, URL: <http://matrix.org/> & <https://github.com/matrix-org/synapse/commit/4f475c7697722e946e39e42f38f3dd03a95d8765>, fist Commit on Aug 12.
- Maurer, M. / Massey, J. L. (1993): Cascade ciphers - The importance of being first, Journal of Cryptology, vol. 6, no. 1, pp. 55–61.
- Maydanchik, Arkady (2007): Data Quality Assessment, Technics Publications, LLC.
- McEliece, Robert J. (1978): A Public-Key Cryptosystem Based On Algebraic Coding Theory, DSN Progress Report. 44: 114–116.
- McGrew, David A. / Viega, John (2005): The Galois/Counter Mode of Operation (GCM), p. 5.
- McManus, Sean / Cook, Mike (2013): Raspberry Pi For Dummies.
- McNoodle Library (2016): Implementation of the McEliece Algorithm in C++, Github.
- Medhi, Deepankar / Ramasamy, Karthikeyan (2007): Network Routing - Algorithms, Protocols, and Architectures, Morgan Kaufmann.
- Medhi, Deepankar / Ramasamy, Karthikeyan (2007): Network Routing: Algorithms, Protocols, and Architectures, Morgan Kaufmann.
- Meister, Andre (2013): Secret Government Document Reveals: German Federal Police Plans to Use Gamma FinFisher Spyware, Netzpolitik.org.
- Mendelsohn, Charles J. (1940): Blaise De Vigenere and The 'Chiffre Carre', Proceedings of the American Philosophical Society, 82 (2).
- Menezes, Alfred J. / van Oorschot, Paul C. / Vanstone, Scott A. (1996): Chapter 7: Block Ciphers, Handbook of Applied Cryptography, CRC Press.
- Mennink, B. / Preneel, B. (2014): Triple and Quadruple Encryption: Bridging the Gaps - IACR Cryptology ePrint Archive, eprint.iacr.org, URL: <http://eprint.iacr.org/2014/016.pdf>.
- Mermin, David (2006): Breaking RSA Encryption with a Quantum Computer: Shor's Factoring Algorithm, Cornell University, Physics, 481-681.
- Micciancio, Daniele / Regev, Oded (2008): Lattice-based cryptography, URL: <https://www.cims.nyu.edu/~regev/papers/pqc.pdf>.

- Miessler, Daniel (2018): Obscurity is a Valid Security Layer, URL: URL: <https://danielmiessler.com/study/security-by-obscurity/>.
- Milgram, Stanley (1967): The Small World Problem, Psychology Today, Ziff-Davis Publishing Company.
- Mockapetris, P. (1987): RFC 1034, Domain Names - Concepts and Facilities, The Internet Society.
- Modadugu, Nagendra / Rescorla, Eric (2003): The Design and Implementation of Datagram TLS, Stanford Crypto Group.
- Momedo (2018): Open Source Mobiler Messenger für kommunale und schulische Zwecke mit Verschlüsselung, Github, URL: <https://momedo.github.io/momedo/> & <https://github.com/momedo/momedo/blob/master/README.md>.
- Moore, Gordon (2015): Gordon Moore - The Man Whose Name Means Progress, The visionary engineer reflects on 50 years of Moore's Law", IEEE Spectrum: Special Report: 50 Years of Moore's Law (Interview), Interviewed by Rachel Courtland.
- Moore, Stephane (2010): Meet-in-the-Middle Attacks, URL: <http://stephanemoore.com/pdf/meetinthemiddle.pdf>.
- Moritz, Hannes (2005): Kryptanalyse des Advanced Encryption Standard, Technische Universität, Wien.
- Muffatto, Moreno (2006): Open Source - A Multidisciplinary Approach, Imperial College Press.
- Nagao, Waka / Manabe, Yoshifumi / Okamoto, Tatsuaki (2005): A Universally Composable Secure Channel Based on the KEM-DEM Framework, TCC:426-444.
- National Institute of Standards and Technology (2013): Electronic Authentication Guideline – NIST Special Publication 800-63-2, URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>.
- Neal, Ryan W. (2013): Edward Snowden Reveals Secret Decryption Programs - International Business Times URL: <https://www.ibtimes.com/edward-snowden-reveals-secret-decryption-programs-10-things-you-need-know-about-bullrun-edgehill>
- Newton, David E. (1997): Encyclopedia of Cryptology, ABC-CLIO.
- Nielsen, Michael A. / Chuang, Isaac (2000): Quantum Computation and Quantum Information, Cambridge: Cambridge University Press.
- Nissenbaum, Helen (1999): The Meaning of Anonymity in an Information Age, The Information Society, 15 (2): 141–44.
- NIST (2001): Announcing the ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST), URL: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>, November 26.
- NIST (2004): Engineering Principles for Information Technology Security, URL: <https://csrc.nist.gov/publications/detail/sp/800-27/rev-a/archive/2004-06-21>.
- NIST / Chen, Lily / Jordan, Stephen / Liu, Yi-Kai / Moody, Dustin / Peralta, Rene / Perlner, Ray / Smith-Tone, Daniel (2016): NISTIR 8105, DRAFT, Report on Post-Quantum Cryptography, URL: <http://csrc.nist.gov/publications/drafts/nistir->

- 8105/nistir_8105_draft.pdf, National Institute of Standards and Technology. February.
- NIST / Office of the Director (2013): Cryptographic Standards Statement, National Institute of Standards in Technology.
- NIST Computer Security Division's (CSD) Security Technology Group (STG) (2013): Block cipher modes, Cryptographic Toolkit, NIST.
- Novak, Matt (2016): Edward Snowden Isn't Right About Everything, URL: <http://www.gizmodo.co.uk/2016/11/edward-snowden-isnt-right-about-everything/>, 18 Nov.
- Obe, Regina / Hsu, Leo (2012): PostgreSQL: Up and Running, O'Reilly.
- OECD (1997): Report of the Workshop on Cryptography Policy, OECD, Paris, 9-10 December.
- OECD (2002): OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, <http://www.oecd.org/dataoecd/16/22/15582260.pdf>
- OpenSSL Committers (2018): OpenSSL Software Foundation, URL: <https://www.openssl.org/community/committers.html>.
- Paar, Christof / Pelzl, Jan (2009): Introduction to Public-Key Cryptography, Chapter 6 of: Understanding Cryptography - A Textbook for Students and Practitioners, Springer, 2009.
- Padua, David (2011): Encyclopedia of Parallel Computing, Volume 4.
- Pandamonium Web Crawler (2015): Github <https://github.com/textbrowser/pandamonium> and Binary at the GoldBug-Project <https://sourceforge.net/projects/goldbug/files/pandamonium-webcrawler/>.
- Partisan Journalism (2014): A History of Media Bias in the United States.
- Patange, Tanmay (2013): How to defend yourself against MITM or Man-in-the-middle attack, URL: <https://hackerspace.kinja.com/how-to-defend-yourself-against-mitm-or-man-in-the-middl-1461796382>
- Patil, Yugandhara / Patil, Sonal (2016): Review of Web Crawlers with Specification and Working, International Journal of Advanced Research in Computer and Communication Engineering, 5(1):4.
- Paul Ducklin (2013): Anatomy of a change – Google announces it will double its SSL key sizes – Naked Security, Nakedsecurity.sophos.com.
- Paul, Eliza (2017): What is Digital Signature- How it works, Benefits, Objectives, Concept, EMP Trust HR.
- PBS (2015): Inside the Court of Henry VIII. Public Broadcasting Service, URL: <https://www.pbs.org/program/inside-court-henry-viii/>, April 8.
- Percival, Colin (2009): Stronger Key Derivation via Sequential Memory-Hard Functions, BSDCan'09 Presentation.
- Perrig, Adrian (2004): Cryptographic Approaches for Securing Routing Protocols URL: dimacs.rutgers.edu/Workshops/Practice/slides/perrig.pdf.
- Perrin, Chad: The CIA Triad, URL <http://www.techrepublic.com/blog/security/the-cia-triad/488>
- Perrin, Trevor (2014): The Noise Protocol Framework, URL: <http://noiseprotocol.org/noise.pdf> & https://github.com/noiseprotocol/noise_spec/commit/c627f8056ffb9c7

- 695d3bc7bafea8616749b073f, Revision 30, 2016-07-14 respective: first commit c627f8056ffb9c7695d3bc7bafea8616749b073f committed Aug 4.
- Peterson, Andrea (2014): Edward Snowden sent Glenn Greenwald this video guide about encryption for journalists. Greenwald ignored it, The Washington Post, May 14.
- Petitcolas, Fabien A.P. / Katzenbeisser, Stefan (2016): Information Hiding, Artech House Publishers.
- Pierce, JR. (1961): An introduction to information theory - symbols, signals and noise, Dover.
- Popescu, Bogdan C. / Crispo, Bruno / Tanenbaum, Andrew S. (2004): Safe and Private Data Sharing with Turtle: Friends Team-Up and Beat the System, in: 12th International Workshop on Security Protocols, Cambridge, UK, April. URL: <http://turtle-P2P.sourceforge.net/turtleinitial.pdf>.
- Popp, Karl Michael (2015): Best Practices for commercial use of open source software. Norderstedt.
- Por, Julianna Isabele (2016): Segurança em primeiro lugar, URL: <https://www.baixaki.com.br/download/goldbug.htm>.
- Possony Stefan T. (2013): Zur Bewältigung der Kriegsschuldfrage: Völkerrecht und Strategie bei der Auslösung zweier Weltkriege, Berlin.
- Postel, J. (1980): User Datagram Protocol, Internet Engineering Task Force.
- Power, Michael (1999): The Audit Society - Rituals of Verification, Oxford, Oxford University Press.
- PRISM Programm (2013): URL: <https://de.wikipedia.org/wiki/PRISM>.
- Privacy International (2017): 10 Human Rights Organisations v. United Kingdom URL: <https://www.privacyinternational.org/node/992>.
- Qt Digia (2015): Qt Digia has awarded GoldBug IM as reference project for Qt implementation in the official Qt>Showroom of Digia: showroom.qt-project.org/goldbug/.
- Quisquater, Jean-Jacques / Guillou, Louis C. / Berson, Thomas A. (1990): How to Explain Zero-Knowledge Protocols to Your Children, Advances in Cryptology – CRYPTO '89, 435, pp. 628–631.
- Rahman, Ashikur / Olesinski, Wlodek / Gburzynski, Paweł (2004): Controlled Flooding in Wireless Ad-hoc Networks, International Workshop on Wireless Ad-Hoc Networks. Edmonton, Alberta, Canada: University of Alberta.
- Raimondo, Mario Di / Gennaro, Rosario / Krawczyk, Hugo (2005): Secure Off-the-Record Messaging, Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Association for Computing Machinery.
- Rasmussen, Rod (2016): The Pros and Cons of DNS Encryption, URL: <http://www.infosecurity-magazine.com/opinions/the-pros-and-cons-of-dns-encryption/>, 14 Sep.
- Rasti, Amir H. / Stutzbach, Daniel / Rejaie, Reza (2006): On the Long-term Evolution of the Two-Tier Gnutella Overlay, URL: <http://www.baroom.org/papers/gi-2006-long-term.pdf>.
- Raymond, Eric S. (2000): The Cathedral & the Bazaar. Musings on Linux and Open Source by an Accidental Revolutionary. O'Reilly & Associates.

- Regev, Oded (2006): Lattice-based cryptography, in: Advances in cryptology (CRYPTO), pp. 131–141.
- Reinert, Manuel (2018): Cryptographic techniques for privacy and access control in cloud-based applications (Englisch), Saarländische Universitäts- und Landesbibliothek, Saarbrücken.
- Rejewski, Marian (1980): An Application of the Theory of Permutations in Breaking the Enigma Cipher, *Applicationes Mathematicae*, 16(4):543–559.
- Rhee, M. Y. (2003): Internet Security - Cryptographic Principles, Algorithms and Protocols, Chichester: Wiley.
- Rhoton, J. (1999): Programmer's Guide to Internet Mail: SMTP, POP, IMAP, and LDAP, Elsevier.
- Risen, James / Poitras, Laura (2013): N.S.A. Report Outlined Goals for More Power, URL: <https://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html>, The New York Times.
- Rittaud, Benoit / Heeffer, Albrecht (2014): The Pigeonhole Principle, Two Centuries before Dirichlet, *Mathematical Intelligencer*, 36 (2): 27–29.
- Rivest, R. L. / Shamir, A. / Adleman, L. (1978): A Method for Obtaining Digital Signatures and Public-key Cryptosystems, *Commun. ACM*. 21 (2): 120–126.
- Robshaw, Matt J. B. (1995): Stream Ciphers Technical Report TR-701, version 2.0, RSA Laboratories.
- Rodriguez-Clark, Dan (2017): Vigenère Cipher, URL: <https://crypto.interactive-maths.com/vigenegravere-cipher.html>, Crypto Corner.
- Rogers, E. M. (1962): Diffusion of Innovation. New York, NY: Free Press.
- Rosenheim, Shawn James (1997): The Cryptographic Imagination, Secret Writing from Edgar Poe to the Internet, Baltimore: Johns Hopkins University Press.
- Russel, J.P. (2003): Continual Improvement Auditing, URL:<http://www.qualitywbt.org/FlexTraining/ASP/content/sections/A12/pdfs/01al-vs-ous.pdf>.
- Sabtu (2014): Free GoldBug Instant Messenger 1.7, URL: <http://bengkelcakra.blogspot.de/2014/12/free-download-goldbug-instant-messenger.html>, 13 December.
- Saini, Hemant Kumar (2014): Backdoor Add-ons - A new way to harbor the data, Munich: GRIN Verlag GmbH.
- Saint-Andre, Peter et. al. (2016): Manifesto: A Public Statement Regarding Ubiquitous Encryption on the XMPP Network, URL: <https://github.com/stpeter/manifesto/blob/master/manifesto.txt>
- Saroiu, Stefan / Gummadi, P. Krishna / Gribble, Steven D. (2002): A Measurement Study of Peer-to-Peer File Sharing Systems. Technical Report # UW-CSE-01-06-02. Department of Computer Science & Engineering. University of Washington. Seattle, WA, USA.
- Satter, Raphael (2017): What makes a cyberattack? Experts lobby to restrict the term, URL: <https://apnews.com/2c25d7da76f4409bae7daf063c071420>.
- Savarese, Chris / Hart, Brian (1999): The Caesar Cipher, URL: <http://www.cs.trincoll.edu/~crypto/historical/caesar.html>.
- Schlienger, Thomas / Teufel, Stephanie (2003): Information security culture-from analysis to change, *South African Computer Journal*, 31: 46–52.
- Schneier, Bruce (1963): E-mail security - how to keep your electronic messages private.

- Schneier, Bruce / Kelsey, Doug / Wagner, David / Hall, Chris / Ferguson, Niels (1999): The Twofish Encryption Algorithm: A 128-Bit Block Cipher, New York City, John Wiley & Sons.
- Schneier, Bruce / Seidel, Kathleen / Vijayakumar, Saranya (2016): A Worldwide Survey of Encryption Products, February 11, 2016 Version 1.0., quoted according to: Adams, David / Maier, Ann-Kathrin (2016): BIG SEVEN Study, open source crypto-messengers to be compared - or: Comprehensive Confidentiality Review & Audit of GoldBug, Encrypting E-Mail-Client & Secure Instant Messenger, Descriptions, tests and analysis reviews of 20 functions of the application based on the essential fields and methods of evaluation of the 8 major international audit manuals for IT security investigations including 38 figures and 87 tables, URL: <https://sf.net/projects/goldbug/files/bigseven-crypto-audit.pdf> - English / German Language, Version 1.1, 305 pages, June 2016.
- Schoenmakers, Berry (1999): A simple publicly verifiable secret sharing scheme and its application to electronic voting", Advances in Cryptology, 1666: 148–164.
- Schulte, Wolfgang (2016): Handbuch der Routing-Protokolle: Eine Einführung in RIP, IGRP, EIGRP, HSRP, VRRP, OSPF, IS-IS und BGP, VDE VERLAG.
- Schwartz, John (2001): Giving Web a Memory Cost Its Users Privacy, URL: <https://www.nytimes.com/2001/09/04/technology/04COOK.html>.
- Security Blog (2014): Secure chat communications suite GoldBug. Security Blog, 25. März, <http://www.hacker10.com/other-computing/secure-chat-communications-suite-GoldBug/>.
- Seggelmann, R. / Tuxen, M. / Rathgeb, E.P. (2012): SSH over SCTP — Optimizing a multi-channel protocol by adapting it to SCTP, Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2012 8th International Symposium on. pp. 1–6.
- Seress, Ákos / Szabó, Tibor (1995): Dense graphs with cycle neighborhoods, Journal of Combinatorial Theory, Series B, 63 (2): 281–293.
- Shamir, Adi (1979): How to share a secret, Communications of the ACM, 22 (11): 612–613.
- Shannon, Claude (1949): Communication Theory of Secrecy Systems, URL: <http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf>, Bell System Technical Journal. 28(4):656–715.
- Shannon, Claude / Weaver, Warren (1963): The Mathematical Theory of Communication, University of Illinois Press.
- Shannon, Claude E. (1948): A Mathematical Theory of Communication, Bell System Technical Journal. 27 (3): 379–423.
- Shannon, Claude E. (1949): Communication Theory of Secrecy Systems, URL: <http://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf>, Bell System Technical Journal. 28 (4): 656–715.
- Sharbaf, M.S. (2011): Quantum cryptography - An emerging technology in network security, 2011 IEEE International Conference on Technologies for Homeland Security (HST), pp. 13–19.
- Shen, X.S. / Yu, H. / Buford, J. / Akon, M. (Eds.) (2010): Handbook of Peer-to-Peer Networking, Springer.

- Shiho Moriai / Yiqun Lisa Yin (2000): Cryptanalysis of Twofish (II), URL: <https://en.wikipedia.org/wiki/PDF>.
- Shor, P.W. (1994): Algorithms for quantum computation: discrete logarithms and factoring, Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE.
- Shoup, Victor / et. al. (2018): A Tour of NTL: Summary of Changes, URL: <https://www.shoup.net/ntl/doc/tour-changes.html>.
- Silverman, Kenneth (1991): Edgar A. Poe - Mournful and Never-Ending Remembrance (Paperback ed.). New York: Harper Perennial.
- SINA (2016): Sichere Inter-Netzwerk Architektur, URL: https://de.wikipedia.org/wiki/Sichere_Inter-Netzwerk_Architektur, Edierung 29.08.
- Sinkov, Abraham (1966): Elementary Cryptanalysis: A Mathematical Approach, Mathematical Association of America.
- Slade, Rob (2008): (ICS)2 Blog, URL: http://blog.isc2.org/isc2_blog/2008/12/cia-triad-versus-parkerian-hexad.html
- Slashdot (2000): Gnutella: <https://en.wikipedia.org/wiki/Gnutella>, & <https://slashdot.org/story/00/03/14/0949234/open-source-napster-gnutella>, 2000.
- Smoke (2017): Documentation of the Android Messenger Application Smoke with Encryption, URL:<https://github.com/textbrowser/smoke/raw/master/Documentation.pdf>, 2017.
- Snowden, Edward (2017): A Manifesto for the Truth - Mass Surveillance Needs Global Solution.
- Sollins, Karen / Masinter, Larry (1994): Request for Comments: 1737: Functional Requirements for Uniform Resource Names, IETF.
- Spot-On (2011): Documentation of the Spot-On-Application, URL: <https://sourceforge.net/p/spot-on/code/HEAD/tree/>, under this URL since 06/2013, Sourceforge, including the Spot-On: Documentation of the project draft paper of the pre-research project since 2010, Project Ne.R.D.D., Registered 2010-06-27, URL: <https://sourceforge.net/projects/nerdd/> has evolved into Spot-On. Please see <http://spot-on.sf.net> and URL: <https://github.com/textbrowser/spot-on/blob/master/branches/Documentation/RELEASE-NOTES.archived>, 08.08.2011.
- Spot-On (2013): Documentation of the Spot-On-Application, URL: <https://github.com/textbrowser/spot-on/tree/master/branches/trunk/Documentation>, Github 2013.
- Spot-On (2014): Documentation of the Spot-On-Application, URL: <https://github.com/textbrowser/spot-on/tree/master/branches/trunk/Documentation>, Github 2014.
- Spot-On (2019): Documentation of the Spot-On-Application, URL: <https://github.com/textbrowser/spot-on/tree/master/branches/trunk/Documentation>, Github 2019.

- Standards for Efficient Cryptography Group (SECG), SEC 1 (2014): Elliptic Curve Cryptography, Version 1.0, September 20, 2000.
- Stanley Milgram (1967): The Small World Problem. In: Psychology Today, URL: http://measure.igpp.ucla.edu/GK12-SEE-LA/Lesson_Files_09/Tina_Wey/TW_social_networks_Milgram_1967_small_world_problem.pdf, ISSN 0033-3107, pp. 60–67, Mai.
- Stebila, Douglas / Mosca, Michele (2016): Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project, Cryptology ePrint Archive, Report 2016/1017.
- Stehlé, Damien / Steinfeld, Ron (2016): Making NTRUEncrypt and NTRUSign as Secure as Standard Worst-Case Problems over Ideal Lattices, Cryptology ePrint Archive.
- Stenberg, Daniel (2015): Curl, 17 years old today, daniel.haxx.se.
- Stevens, W. Richard (1996): TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols.
- Stewart, Ian (1990): Does God Play Dice? - The Mathematics of Chaos, Blackwell Publishers.
- Stollznow, Karen (2014): Eavesdropping: etymology, meaning, and some creepy little statues, KarenStollznow.com.
- Stross, Randall (2015): Theater of the Absurd at the T.S.A., URL: <https://www.nytimes.com/2006/12/17/business/yourmoney/17digi.html>, The New York Times.
- Sutherland, Denise / Koltko-Rivera, Mark (2009): Cracking Codes and Cryptograms For Dummies, John Wiley & Sons.
- Talia, Domenico / Trunfio, Paolo (2010): Enabling Dynamic Querying over Distributed Hash Tables, Journal of Parallel and Distributed Computing, 70(12):1254–1265.
- Tamblyn, Thomas (2016): What Is The "Pegasus" iPhone Spyware And Why Was It So Dangerous?", The Huffington Post.
- The United Nations / Office of the High Commissioner of Human Rights (2014): What are human rights?.
- Theisen, Michaela (2015): GoldBug Instant Messenger - Beliebte Software, Sicherer Instant Messenger, URL: https://www.freeware-base.de/freeware-zeige-details-28142-GoldBug_Instant_Messenger.html.
- Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein (2001): Introduction to Algorithms, 2. Auflage, MIT Press, Cambridge (Massachusetts) 2001.
- Thomas, Stephen A. (2000): SSL and TLS essentials securing the Web, New York: Wiley.
- Trachtenberg, Ari (2014): Say it Ain't So - An Implementation of Deniable Encryption", Blackhat Asia, Singapore.
- Tsikerdekis, Michail (2013): The effects of perceived anonymity and anonymity states on conformity and groupthink in online communities: A Wikipedia study, Journal of the Association for Information Science and Technology, 64 (5): 1001–1015.
- Tsiounis, Yiannis / Yung, Moti (1998): On the Security of ElGamal Based Encryption, Public Key Cryptography, 117–134.

- Tuxen, Michael / Stewart, Randall R. (2013): UDP Encapsulation of Stream Control Transmission Protocol (SCTP), Packets for End-Host to End-Host Communication, IETF.
- Tuohy, William (2007): America's Fighting Admirals: Winning the War at Sea in World War II, MBI Publishing Company.
- Tur, Henryk / Computerworld (2018): GoldBug Secure Email Client & Instant Messenger, <https://www.computerworld.pl/ftp/goldbug-secure-email-Client-instant-messenger.html>, January 11.
- Turing, Alan (1948): Intelligent Machinery; reprinted in: Turing, A. M. (1996): Intelligent Machinery - A Heretical Theory, *Philosophia Mathematica*, 4 (3): 256.
- Turing, Alan (1950): Computing Machinery and Intelligence, *Mind*. 49 (236): 433–460.
- Turner, Dawn (2016): Major Standards and Compliance of Digital Signatures - A World-Wide Consideration, Cryptomathic.
- Turner, Dawn M. (2016): Digital Authentication: The Basics, Cryptomathic, URL: <http://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics>.
- United Nations (2015): E-Government Survey 2012: E-Government for the People, Un.org.
- Urdaneta, Guido / Pierre, Guillaume / van Steen, Maarten (2011): A Survey of DHT Security Techniques, *ACM Computing Surveys* 43(2).
- Van den Hoooff, Jelle / Lazar, David / Zaharia, Matei / Zeldovich, Nickolai (2015): Vuvuzela: Scalable Private Messaging Resistant to Traffic Analysis, URL: <https://davidlazar.org/papers/vuvuzela.pdf>, 08.09.
- van Tilborg, Henk C. A. / Jajodia, Sushil (Eds.) (2011): Encyclopedia of Cryptography and Security, Springer.
- Vigenère, Blaise de (1586): Traicté des Chiffres, ou Secretes Manieres d'Ecrire [Treatise on ciphers, or secret ways of writing] (in French), Paris, France: Abel l'Angelier.
- Vinberg, Ernest Borisovich (2003): A Course in Algebra, American Mathematical Society, p. 3.
- Vincentas (2013): Keystroke Logging in SpyWareLoop.com, Spyware Loop.
- Vu, Quang H. / et al. (2010): Peer-to-Peer Computing - Principles and Applications, Springer.
- Waldrop, M. Mitchell (1992): Complexity - The Emerging Science at the Edge of Order and Chaos, New York.
- Wallace, Kathleen A. (1999): Anonymity, Ethics and Information Technology, 1: 23–35.
- Washington, L. (2003): Elliptic Curves - Number Theory and Cryptography, Chapman & Hall / CRC.
- Wayner, Peter (2009): Disappearing, cryptography 3rd Edition: information hiding: steganography & watermarking. Amsterdam: MK/Morgan Kaufmann Publishers.
- Welchman, Gordon (1984/1997): The Hut Six Story: Breaking the Enigma Codes, p. 78.
- Weller, Jan (2013): Testbericht zu GoldBug für Freeware, Freeware-Blog, URL: <https://www.freeware.de/download/goldbug/>.
- Wiesner, Stephen (1983): Conjugate coding, *ACM SIGACT News*, 15(1):78–88.
- Wikipedia.org (2019): Referenced keywords and descriptions and there found further references and bibliography, www.wikipedia.org.

- Willmott, H. P. (2005): The Great Day of Wrath: 25 October 1944, The Battle of Leyte Gulf: The Last Fleet Action, Indiana University Press.
- Wouters, P. (2016): RFC 7929 - DNS-Based Authentication of Named Entities (DANE) Bindings for OpenPGP URL: <https://datatracker.ietf.org/doc/rfc7929/>, August.
- Yao, Andrew (1982): Protocols for secure communications, Proc. 23rd IEEE Symposium on Foundations of Computer Science (FOCS '82), pp. 160–164.
- Yeung, R.W. (2002): A First Course in Information Theory Kluwer Academic/Plenum Publishers.
- Ylonen, Tatu (2001): SSH trademarks and the OpenSSH product name, openssh-unix-dev (Mailing list). MARC.
- Zantour, Bassam / Haraty, Ramzi A. (2011): I2P Data Communication System, Proceedings of ICN 2011: The Tenth International Conference on Networks (IARIA), pp:401–409.
- Zeng, Marcia / Qin, Jian (2016): Metadata, Facet.
- Zhang, Yupu / Rajimwale, Abhishek / Arpacı-Dusseau, Andrea C. / Arpacı-Dusseau, Remzi H. (2014): End-to-end Data Integrity for File Systems: A ZFS Case Study, Computer Sciences Department, University of Wisconsin.
- Zhen, Jane (2003): Preventing Replay Attacks for Secure Routing in Ad Hoc Networks; in: Ad-Hoc, Mobile, and Wireless Networks, Lecture Notes in Computer Science, 2865, pp. 140–150.

Index of Keywords

2

2-Way-Calling 117

A

Access Control 62

Adaptive Echo 62, 63, 66, 120

AddRoundKey 66

Advanced Encryption Standard

63

AE 62, 66, 120, 147

AES 63, 64, 65, 90, 96, 115, 126, 145, 147, 168, 180, 184, 214, 241, 252, 260, 313, 351, 352

AE-Token 66

Algorithm 64, 66, 67, 81, 85, 90, 92, 102, 104, 108, 112, 113, 114, 118, 119, 123, 125, 127, 128, 133, 143, 145, 152, 153, 155, 160, 161, 168, 175, 182, 191, 193, 196, 205, 217, 219, 223, 225, 230, 232, 239, 240, 249, 252, 253, 260, 263, 266, 269, 275, 280, 281, 282, 283, 285, 287, 297, 311, 313, 316, 317, 330, 331, 337, 345, 348, 351

Alias 316

Alice and Bob 68

Android 82, 260, 316, 317

Anonymity 69

Anonymous Message 70

Answer Method 70

Assessment 62, 198, 343

Asymmetric 71, 72, 113, 124, 125, 126, 129, 135, 145, 152, 160,

161, 176, 182, 196, 211, 218, 223, 239, 240, 241, 284, 331

Asymmetric Calling 71, 117

Asymmetric Encryption 71

Attack 73

Attacker 70, 94, 114, 133, 160, 215, 217, 222, 224, 225, 232, 244, 246, 261, 265, 269, 291, 313, 314, 325, 338, 347

Audit 74, 77, 84, 339

Authentic Channel 301

Authentication 77, 78, 79, 81, 120, 122, 135, 166, 168, 170, 174, 179, 191, 193, 211, 212, 215, 217, 225, 230, 244, 256, 258, 260, 264, 268, 281, 300, 310, 314, 319, 338, 339, 341, 361

Authenticity 78, 90, 135, 230, 343, 359

Authorization 62, 79, 146

AutoCrypt 80

Availability 80

Axolotl Ratchet 312

B

B.A.T.M.A.N. 243

Backdoor 81, 291

Beyond Cryptographic Routing 131

Big Seven Study 84

Bijection 89

Biometric 168

Biometric Passport 85

Birthday Problem 87

Bletchley Park 113, 335, 336, 350

Blinding Techniques 88

Block Cipher 64, 90, 91, 97, 105, 180, 222, 226, 246, 324, 336, 345, 351

Bluetooth 92

Bombe 335

Botan 92

Bouncy Castle 93

Boundless Informant 306

Broadcast 94, 160, 272

Browser 134, 138, 207, 209, 311, 337, 340, 341

Brute-Force Attack 94, 114, 215, 224, 289

BSD 92

Bullrun 95, 292, 306

Butterfly Effect 101

Button 96

Buzz 96, 174, 209, 231

C

C# 93

C++ 92, 252

Caesar Cipher 98, 99, 100, 297, 357

Capsule 143, 145, 147, 154

Care of 97

Censorship 174, 176, 179, 241, 350

Certificate Authority 100

Channel 71, 80, 88, 94, 112, 126, 133, 135, 143, 161, 176, 189, 200, 208, 211, 219, 227, 231, 242, 257, 258, 280, 296, 311, 319, 330, 361

Chaos 101

Chat Server 292

Cipher 63, 64, 90, 91, 92, 97, 98, 99, 102, 104, 105, 123, 128, 145, 146, 154, 155, 161, 197, 218, 223, 226, 249, 269, 295, 297, 323, 345, 351, 356

Cipher Block Chaining 91, 97

Cipher Feedback Mode 92

Ciphertext 64, 91, 97, 98, 104, 105, 113, 123, 128, 133, 145, 146, 154, 156, 162, 192, 196, 198, 217, 221, 223, 232, 246, 253, 259, 269, 295, 324, 330, 358

Ciphertext Stealing 105

Circuit 64, 108, 156, 248, 288, 326

Citizens 150, 169, 233, 328

Client-Side Encryption 105

Cloud 81, 126, 170, 192

C-Mail 106

Code 64, 75, 82, 84, 93, 94, 95, 98, 100, 102, 104, 126, 141, 161, 185, 191, 211, 219, 221, 230, 256, 264, 269, 282, 301, 314, 338, 358, 393

Code-Based Cryptography 276

Codebook 91, 161, 219

Collision Attack 106, 346

Colossus computers 113

Communication 71, 79, 80, 85, 89, 107, 112, 122, 145, 151, 155, 159, 162, 179, 180, 189, 193, 195, 199, 203, 209, 212, 219, 244, 256, 268, 271, 284, 286, 288, 292, 310, 312, 316, 317, 321, 340, 344, 361

Complexity 87, 106, 107, 112, 288, 324

Computer Security 68, 207, 230, 244

Confidential Channel 301

Confidentiality 90, 109, 122, 167, 198, 199, 221, 277, 320, 331, 343, 344

Configuration 109

Congestion Control 109, 143, 300, 354

Continuous Improvement 109,
110
Cookie 340, 341
Corrective Action 111
CO-TRAVELER Analytics 306
Crawler 111
Credential 71, 78, 111, 115, 134,
204, 208, 230, 328
Cryptanalysis 112, 133, 262, 311
Crypto Party 85
Crypto-Agility 114
Cryptogram 114, 115, 122, 149,
253
Cryptographic Calling 71, 115,
116, 166, 176, 208, 319, 330,
352, 361
Cryptographic Discovery 117,
118, 164
Cryptographic DNA 118
Cryptographic Hash 106, 171, 172,
190, 191, 214, 222, 226, 228,
230, 231, 263, 265, 288, 314
Cryptographic Primitives 114, 119,
227, 313
Cryptographic Protocol 119
Cryptographic Routing 120
Cryptographic Token 62, 66, 120
Cryptographic Torrents 121
Cryptography 68, 88, 93, 94, 102,
112, 117, 120, 122, 124, 125,
132, 133, 135, 149, 152, 161,
171, 181, 182, 186, 190, 196,
200, 204, 205, 209, 212, 215,
217, 218, 223, 227, 229, 239,
241, 244, 247, 252, 253, 256,
259, 261, 268, 269, 270, 275,
280, 283, 285, 290, 299, 310,
311, 312, 317, 323, 330, 333,
337
Cryptology 122
CrypTool 125
CryptoPad 123

Crypto-Party 124
CSEK 126
CSPRNG 290
Curve25519 313
Customer Supplied Encryption Keys 126

D

Data Encryption Standard 64
Data Exposure 127
Data Integrity 74, 122, 191, 206,
231, 337, 344
Data Validation 128
Database 128, 353
Database Encryption 128
Datagram Transport Layer Security 139, 338
Decentralized 130, 185
Decentralized Computing 130
Delta Chat 130
Democratization of Encryption 132
Deniability 133, 256, 270
DES 64, 133, 246, 345
Deterministic Random Bit Generator 281
DFA 133
DHT 134
Dictionary Attack 95, 215
Differential Fault Analysis 133
Diffie-Hellman 125, 152, 153, 161,
166, 212, 214, 220, 227, 260,
302, 310, 313
Digest 135, 145, 170, 190
Digest Access Authentication 134
Digital Certificate 282
Digital Signature 68, 73, 125, 135,
152, 179, 253
Dirichlet's Box Principle 268

- Distributed 92, 106, 130, 134, 138, 160, 171, 179, 221, 230, 255, 284, 290, 308, 362
- Distributed Hash Table** 134
- DNS** 137
- Documented Information** 138
- Domain Name System** 137
- Dooble Web Browser** 138
- Double Ratchet Algorithm 255
- DRBG 281, 291
- DTLS** 139, 162, 338
- E**
- E2EE** 167
- Eavesdropping** 123, 139, 140, 141, 166, 216, 244, 245, 257, 275, 280, 286, 302, 303
- ECC** 125, 152, 287
- ECDH** 153
- ECDLP** 153
- ECDSA** 153, 290
- ECHELON** 141, 142, 328
- Echo** 62, 80, 94, 117, 120, 131, 143, 144, 146, 147, 148, 154, 164, 167, 169, 173, 189, 209, 227, 241, 243, 284, 300, 316, 321, 322, 325, 354
- Echo Accounts** 146
- Echo Match** 143, 146, 154
- Echo Protocol** 143, 144
- Echo Public Key Share** 161
- Echo Public Key Sharing Protocol** 80, 94, 227
- Echo-Grid** 147
- Echo-Network** 94, 117, 131, 143, 148, 161, 167, 204, 243
- Edgar Allan Poe** 122, 149, 185
- Education 194
- Edward Snowden 124, 234, 277, 328, 330
- EEE** 164
- E-Government** 150, 151
- Electronic Mail** 136, 207, 317
- ElGamal** 85, 152
- Elliptic Curve** 152, 153, 205, 223, 276, 283
- Elliptic-Curve Cryptography** 152
- E-Mail** 76, 80, 84, 97, 106, 130, 154, 184, 197, 203, 204, 232, 252, 256, 258, 272, 273, 274, 284, 295, 316, 321, 347
- E-Mail-institution** 154
- Encapsulation** 154, 196, 249
- Encipher** 102, 245, 358
- Encode** 88, 95, 102, 104, 147, 171, 172, 286
- Encrypt Then Mac** 162
- Encryption** 63, 65, 71, 72, 75, 80, 81, 84, 88, 90, 91, 94, 95, 96, 98, 102, 104, 105, 111, 114, 115, 119, 122, 124, 126, 127, 131, 132, 135, 143, 145, 152, 154, 155, 159, 161, 162, 164, 165, 167, 169, 170, 174, 176, 184, 195, 196, 198, 199, 204, 208, 211, 217, 218, 219, 222, 224, 228, 232, 239, 240, 241, 246, 247, 249, 252, 253, 255, 256, 258, 259, 260, 261, 263, 264, 266, 268, 269, 273, 282, 283, 284, 287, 291, 295, 296, 297, 299, 303, 309, 310, 312, 317, 319, 321, 324, 329, 330, 337, 339, 345, 351, 352, 357, 361
- Encryption Suite** 321
- End-to-End** 71, 115, 160, 167, 176, 180, 184, 208, 242, 247, 255, 312, 319, 330, 352, 361
- Enigma** 155, 157, 158, 221, 335, 336
- Entity Authentication** 120

Entropy 159, 200, 212, 222, 224, 229, 290

Ephemeral Keys 71, 160, 176, 208, 284, 300, 312

EPKS 80, 94, 131, 227

EPKS Protocol 161

Espionage 141, 326, 330

Euclid 66

Exponential Encryption 164, 167

Exponential Key Exchange 166

Exponentially 95

Extensible Messaging and Presence Protocol 361

F

F2F 179, 350

Facial Recognition System 168

Factorization 113, 123, 153, 275, 283, 310

FAIRVIEW 306

Feistel network 64, 351

Fiasco Forwarding 169, 208

Fiasco Keys 166, 169

File-Encryptor 170

File-Sharing 131, 132, 170, 175, 209, 255

FinFisher 172

Fingerprint 168, 171, 338

FinSpy 172

FireChat 173

Firewall 146, 174, 198

First Mobile McEliece Messenger 317

Flooding 175

Flooding Network 167

Folk Theorem 250

Footprint 118

Forward Secrecy 117, 160, 175, 176, 208

Forward-Secrecy-Calling 117, 176

Freedom 176

Freenet 179, 255

Freifunk 243

Friends 80, 131, 144, 147, 154, 179, 180, 260, 294, 316

Friend-to-Friend 131, 179, 255, 350

Full Echo 143, 179, 189

G

Galois 152, 180

GCM 180

Gemini 180, 181, 241

Genie 306

Global Surveillance 277

GnuPG 182, 229, 359

Gnutella 182

Going the Extra Mile 182

GoldBug 70, 76, 80, 84, 104, 149, 184, 252

Goldbug-feature 184

Goppa Code 185, 239

Governance 127, 151, 272, 285

Government 63, 82, 141, 150, 155, 169, 195, 207, 277, 326, 330, 345

GPG 73, 160, 182

Graph-Theory 143, 147, 148, 164, 167, 175, 186, 187, 251, 354

Great Firewall Of China 174

Grid 62, 107, 130, 147, 148, 186, 188

Group Chat 96, 173, 188, 209, 231, 321

Grub 111

GUI 96, 149, 151, 185, 189

H

HackingTeam 292

Half Echo 143, 189

Hansel and Gretel 62

Hardware 79, 273
Hash Function 87, 135, 146, 171, 190, 191, 226, 228, 230, 260, 265, 280, 314, 336
Hash-Based Cryptography 276
HMAC 174, 191, 313, 314
Homomorphic Encryption 125, 192, 193, 228, 233
Homomorphic Secret Sharing 193
Homomorphism 192, 193, 210
HRNG 289
HTTPS 104, 120, 135, 144, 148, 193, 312, 340, 354
Human Rights 177, 193, 277
Hybrid Encryption 125, 182, 196

I

Identification 77, 111, 197, 308, 328
Identity 69, 85, 89, 112, 117, 134, 162, 215, 250, 257, 264, 268, 282, 319, 338, 359
IM 75, 151, 203, 361
IMAP 130, 154, 197, 258, 273
Impersonator 197, 313
Information Science 200
Information Security 198, 199, 344
Information Systems 74, 112, 201
Information Technology 74, 252
Information Theory 159, 199, 224, 287
Information-Theoretic Security 199
Innovation 202
Insecure Channel 302
InSiTo 93
Instant Messaging 84, 140, 188, 203, 207, 260, 312, 337, 361
Instant Perfect Forward Secrecy 176, 208, 284

Institution 154, 204
Integer Factorization 205
Integrity 206, 230, 344
interception 141, 303, 326
Internet 106, 111, 126, 137, 150, 169, 174, 177, 193, 195, 197, 200, 203, 207, 244, 251, 258, 263, 272, 274, 277, 296, 317, 321, 326, 331, 340, 352, 354, 363
Internet Relay Chat 209
Internet Security 207
invention 80, 200, 203, 220, 301
IPFS 176, 208
IRC 209
Iris Recognition 168
Isomorphism 209
Iterated Function 210

J

Java 93, 210, 362
J-PAKE 211, 212
Juggernaut Keys 166, 211, 222
Juggernauts 211, 245
Juggernaut PAKE Protocol 212
Juggling 212

K

KDF 214
Keccak 126, 309
Kerberos 215, 310
Kerckhoffs' Principle 211, 216, 217, 223
Kernel 96, 117, 149, 184, 216, 360
Ketje 309
Key 64, 68, 71, 80, 86, 89, 90, 91, 92, 94, 99, 105, 108, 112, 115, 118, 120, 124, 126, 127, 128, 133, 134, 136, 145, 146, 152, 155, 156, 161, 166, 168, 169,

171, 175, 176, 180, 182, 191,
196, 200, 204, 208, 211, 212,
214, 215, 216, 217, 218, 224,
227, 228, 231, 240, 241, 245,
246, 249, 253, 255, 258, 259,
260, 263, 266, 269, 273, 275,
279, 282, 284, 285, 289, 290,
293, 295, 296, 299, 301, 302,
310, 312, 314, 317, 320, 323,
330, 335, 338, 343, 345, 346,
351, 358, 359

Key Agreement 120, 152, 160,
166, 175, 212, 310
Key Derivation Function 94, 214,
289, 310
Key Encryption Key 159
Key Establishment 160, 161, 219
Key Exchange 80, 126, 152, 153,
161, 166, 182, 212, 214, 218,
227, 260, 285, 302, 312
Key Exchange Problem 161, 219,
285
Key Length 223, 260, 346
Key Management 218
Key Size 64, 118, 153, 223, 276,
346

Key Stretching 215, 224
Key Transfer Problem 211
Keyak 309
Keyboard 156, 218, 226
Keystroke Logging 226
KeySyc 227

L

Lattice Graph 186
Lattice-Based Cryptography 126,
227, 252, 276, 287
Libcurl 229
Liberty 69, 194
Libgcrypt 229
LibSpotOn 96, 229

LineageOS 69
Listener 146, 230, 360
Login 70, 230

M

MAC 145, 160, 162, 191, 230
Magnet 96, 118, 154, 231, 232,
259, 295, 322
Magnet-URI 96, 118, 154, 231,
232, 295, 322
Mailbox 154
Malleability 232
Man-in-the-Middle 79, 244, 246,
294
Manipulation 193, 200, 312
Mass Surveillance 233
Matrix 236
Matryoshka Dolls 237
McEliece 126, 186, 197, 239, 240,
263, 287, 317
McNoodle Library 240
Measurement 240
Media Bias 240
Meet-in-the-Middle 244, 246,
258, 286, 319, 346
MELODICA 241
Mesh Network 149, 175, 242
Message 62, 68, 70, 89, 91, 99,
105, 113, 117, 120, 122, 129,
132, 135, 137, 139, 143, 144,
145, 146, 147, 154, 155, 156,
160, 161, 164, 166, 170, 185,
189, 190, 191, 197, 203, 215,
217, 221, 224, 230, 232, 245,
247, 249, 253, 256, 261, 269,
270, 273, 284, 300, 310, 314,
315, 322, 325, 335, 338, 344,
357, 358, 361
Metadata 244
MITM 244, 246
Mix Networks 247

- MixColumns 65
Monitoring 247
Moore's Law 248
Morphism 210
Mosaic 248
Multi Encrypted Long Distance Calling 241
Multicast Key 159
Multi-Encryption 133, 145, 196, 246, 249
Multivariate Cryptography 276
Mutual Authentication 250

N

- National Institute of Standards and Technology 63, 78, 153, 251
National Security Agency 153, 305, 328
Ncat 251
Neighbor 97, 121, 143, 149, 164, 251, 300
Netcat 251
Network 64, 66, 78, 94, 105, 107, 109, 117, 131, 135, 137, 139, 141, 144, 146, 148, 154, 164, 167, 174, 179, 182, 193, 197, 203, 207, 209, 215, 222, 247, 251, 255, 257, 260, 263, 268, 284, 293, 294, 308, 315, 328, 329, 331, 337, 340, 345, 347, 350, 352, 353, 360, 361
Neuland 251
New Era of Exponential Encryption 164
Niederreiter Cryptosystem 239
NIST 63, 78, 84, 91, 153, 251, 265, 291, 309, 336, 343, 346
Node 62, 66, 80, 120, 134, 143, 146, 149, 154, 164, 179, 204, 242, 247, 263, 272, 300, 325, 360

- NOVA** 252
NSA 124, 153, 233, 277, 291, 328, 329, 330
NSO Group 265
NTL 252
NTRU 85, 197, 228, 252
Null Cipher 253
Number Theory 126, 205, 252, 254
Number Theory Library 252
Nutch 111

O

- Obfuscation** 95, 127
Obscurity 304
OFF System 255
Off-the-Record 260
OMEMO 255
One-Time Pad 89, 123, 199, 259, 324
One-Time-Magnet 259
Open Source 75, 84, 111, 138, 223, 240, 252, 256, 257, 285, 316
OpenPGP 73, 130, 182, 221, 249, 256, 266, 351, 359
OpenSSH 257
OpenSSL 138, 257, 346
Opportunistic Encryption 258
OTM 259
OTP 89, 259, 324
OTR 84, 167, 260, 312
Owner-Free File System 255
Ozone 260, 317

P

- P2P** 130, 144, 154, 179, 255, 284, 350, 362
Padding 261
Pandamonium 111, 262

- Passphrase** 115, 124, 181, 214, 224, 260, 263, 299, 310, 319, 352
- Pass-through** 263, 264
- Password** 66, 70, 94, 115, 126, 134, 145, 184, 198, 211, 212, 214, 224, 230, 252, 263, 264, 265, 272, 288, 299, 310, 312, 319, 320, 338, 344
- Patch-Points** 264
- PDCA** 76, 110
- Peer-to-Peer** 130, 171, 175, 179, 182, 203, 204, 255, 284, 321, 350, 362
- Pegasus** 264
- Pepper** 265
- Perfect Forward Secrecy** 175, 176
- Performance** 266
- Permutation** 64, 89, 90, 309
- PGP** 152, 160, 172, 182, 256, 305, 359
- Pigeonhole Principle** 87, 267
- PKI** 71, 72, 86, 115, 124, 268, 283, 359
- Plaintext** 64, 70, 81, 91, 92, 97, 98, 99, 104, 105, 113, 123, 132, 146, 147, 154, 155, 162, 192, 196, 215, 217, 223, 232, 241, 246, 253, 259, 261, 269, 296, 323, 330, 346, 357, 358
- Plausible Deniability** 270
- Point-to-Point** 203, 271
- Policy** 79, 110, 198, 218, 272, 345
- POP3** 130, 154, 272, 273
- POPTASTIC** 130, 203, 273, 274, 295
- Post Office Protocol** 272
- PostgreSQL** 274
- Post-Quantum Cryptography** 126, 227, 228, 239, 275, 276, 287, 311
- Prekeys** 313
- Prime Factorization** 205
- Prime Numbers** 205, 254, 299
- PRISM** 276, 306
- Privacy** 69, 86, 89, 96, 106, 138, 152, 169, 182, 192, 193, 194, 234, 256, 277, 279, 280, 326, 337, 342, 343
- Privacy Amplification** 279
- Private Key** 73, 115, 128, 136, 137, 160, 161, 175, 219, 245, 280, 283
- Private Servers** 132, 281
- PRNG** 281, 289
- Probability Theory** 87
- Protocol** 62, 80, 82, 89, 117, 119, 120, 126, 130, 135, 139, 143, 144, 147, 148, 154, 161, 164, 166, 172, 175, 193, 197, 199, 203, 207, 209, 211, 212, 215, 218, 227, 241, 243, 250, 255, 257, 258, 260, 272, 274, 284, 294, 300, 302, 310, 312, 317, 318, 321, 323, 325, 331, 333, 337, 352, 354, 361
- Pseudo-Random Number Generator** 152, 281, 290, 291, 333
- Public Key** 68, 73, 80, 113, 120, 124, 129, 152, 153, 160, 161, 166, 171, 182, 196, 206, 211, 212, 216, 219, 220, 227, 245, 247, 249, 252, 261, 268, 275, 280, 283, 293, 295, 299, 310, 311, 319, 331, 338, 359
- Public Key Certificate** 282
- Public Key Cryptography** 68, 113, 220, 283
- Public Key Infrastructure** 268
- Pure Forward Secrecy** 284

Q

- QKD** 286
Qt 111, 138, 284
Quantum Communication 285
Quantum Computing 154, 199, 205, 275, 285, 287, 288
Quantum Cryptography 126, 275, 285, 288
Quantum Information Science 285, 287
Quantum Key Distribution 285
Quantum Logic Gate 288
Qubits 288, 310

R

- Rainbow Table** 288, 299
Random 81, 89, 90, 91, 92, 102, 117, 152, 155, 159, 166, 197, 200, 215, 225, 247, 255, 259, 280, 281, 289, 299, 309, 314, 324, 332, 339, 341
Random Number Generator 289, 333
Randomness 289
Raspberry Pi 69, 292
Reliability Theory 80
Remote Control Systems 293
Replay Attack 117, 135, 216, 293
REPLEO 80, 227, 293
Requirement 294
RetroShare 84, 131, 204, 350
Review 74, 295
Rewind 295
RFC 144, 162, 182, 192, 197, 249, 256, 258, 283, 300, 317, 338, 345, 351, 352, 361
Rights 62, 123, 127, 169, 177, 234, 278
Rijndael 63
RNG 289

- Robotics** 168
Rook's graph 186, 188
Rosetta Stone 296
Rosetta-CryptoPad 123, 295
ROT13 98, 297, 298
Round Function 64, 351
Routing 62, 120, 131, 144, 175, 243, 247, 298
RSA 73, 85, 125, 145, 153, 172, 205, 220, 227, 241, 287, 291, 299, 311

S

- S/MIME** 73
Salsa20 336
Salt 215, 265, 289, 299
SCTP 300
SECRED 118
Secret 81, 89, 96, 122, 129, 133, 136, 141, 153, 160, 175, 185, 191, 196, 211, 212, 214, 217, 219, 231, 259, 264, 265, 299, 301, 302, 319, 323, 328, 329, 331, 332, 335, 337, 363
Secret Sharing 120
Secret Splitting 319
Secret Streams 211, 222, 300, 319
Secure by Design 301
Secure Channel 301
Secure Communication 303
Security 62, 70, 73, 79, 82, 84, 86, 90, 93, 99, 109, 111, 112, 114, 119, 122, 127, 135, 139, 141, 152, 153, 162, 168, 174, 177, 179, 180, 217, 218, 223, 227, 234, 246, 249, 251, 253, 256, 257, 258, 263, 266, 275, 277, 280, 283, 286, 291, 294, 297, 301, 302, 304, 312, 324, 328, 330, 337, 338, 342, 343, 344, 346

- Security Hole 127
Security through Obscurity 304
Selectors 305
Sensitive 101, 127, 129, 134, 199, 221, 277, 319, 339, 342, 344, 352
Server 69, 75, 80, 82, 92, 93, 105, 117, 130, 131, 134, 146, 148, 161, 175, 197, 203, 209, 216, 230, 247, 250, 257, 260, 272, 274, 281, 292, 308, 312, 316, 317, 337, 341
Serverless 204
Session 71, 78, 115, 167, 175, 182, 208, 213, 221, 308, 310, 313, 337
Session History 308
Session Key 159
Session Management 308
SHA-1 172, 260, 309
SHA-2 172, 309
SHA-3 172, 191, 309, 336
SHA-512 281
Shared Secret 310
ShiftRows 65
Shor's Algorithm 310
Side-Channel Attack 88, 112, 311
Signal Protocol 312
Signature 89, 135, 137, 153, 154, 217, 281, 282, 287, 290, 338
Silence 177
Simple Mail Transfer Protocol Secured 317
Simulacra 313
SipHash 314, 316
Small World Phenomenon 314
Smoke 117, 131, 169, 173, 211, 212, 222, 260, 280, 316, 317
Smoke Alias 316
Smoke Crypto Chat 316
SmokeStack 69, 117, 170, 260, 281, 316, 317
SMP 117, 211, 222, 245, 300, 318, 319
SMP-Calling 117, 319
SMTPS 258, 317
Socialist Millionaire Protocol 211, 317, 319
Software 71, 74, 79, 185, 222, 316, 343
Source Code 256, 305
Splitted Secret 319
Sponge Construction 309
Spot-On 70, 71, 80, 94, 97, 117, 118, 123, 143, 148, 149, 161, 170, 174, 180, 184, 189, 197, 208, 211, 222, 241, 248, 259, 262, 263, 264, 273, 284, 300, 321, 360
Spot-On Encryption Suite 321
Sprinkling Effect 118, 300
SQLite 138, 321
SSL 92, 145, 147, 193, 257, 281, 291, 317, 337
StarBeam 259, 295, 322
StarBeam-Analyzer 322
Steganography 322
Stream Cipher 92, 232, 309, 323
Stream Control Transmission Protocol 300
Strengths 75, 133
Substitution 64, 65, 90, 98, 294, 297, 356
Super-Echo 325
Supersingular Elliptic Curve Isogeny Cryptography 276
Surveillance 141, 168, 235, 279, 303, 326, 327, 329, 340
Surveillance, global 328
Symmetric Calling 117, 330
Symmetric Encryption 120, 128, 331

Symmetric Key 64, 182, 196, 220, 223, 249, 260, 287, 310, 312, 331, 336, 345

Symmetric Key Quantum Resistance 276

System Integrity 206

T

Tabula Recta 103, 357

TCP 139, 143, 197, 251, 260, 272, 281, 300, 317, 331, 354

TEA 336

Technology 74, 81, 85, 92, 123, 151, 168, 188, 203, 245, 252, 287, 303, 326, 341, 342, 345

Tempora 306

The Ali Baba Cave 332

Theorem 267, 286

Third Party 74, 79, 111, 216, 218, 286, 303, 334

Threefish 336

Timing 337

TLS 73, 92, 120, 135, 139, 145, 147, 162, 193, 245, 250, 257, 281, 283, 337, 361

Toffoli Gate 288

Token 62, 66, 78, 338

Tor 340

Transformation 64, 90, 99, 151, 193, 217, 324, 330, 351

Transmission 143, 153, 169, 171, 203, 208, 264, 269, 280, 287, 293, 295, 299, 301, 317, 323, 338, 352, 355

Transmission Control Protocol

300, 331

Transport Layer Security 120, 193, 257, 283, 337

Transposition 65

Triad of CIA 342

Triple DES 133, 246, 345

Trojan Horse 82, 346

Trusted 112, 131, 161, 174, 215, 220, 245, 294

Trusted Execution Environment 184

Turing Machine 348

Turtle-Hopping 350

Twofish 351

Two-Way Authentication 250

Two-Way-Calling 352

U

UDP 139, 251, 300, 331, 352

Uniform Resource Identifier 353, 354

Uniform Resource Locator 353

Uniform Resource Name 354

Untrusted 174

URI 96, 353, 354

URL 85, 229, 262, 321, 341, 353

URL data-base 321

URL-Distiller 353

URN 354

User Datagram Protocol 300, 331, 352

V

Vapor Protocol 354

VEMI 356

Vigenère Cipher 98, 356

Virtual E-Mail Institution 356

Virtual Keyboard 355

VPN 139, 263

Vulnerability 79, 86, 114, 141, 167, 199, 269, 301, 304, 305, 346

W

Weaknesses 75, 95, 111, 112, 133, 269, 311, 361
Web-Crawler 262
Web-of-Trust 131, 146, 359
Wide Lanes 360
Wikipedia 253, 353
Wiretapping 258

X

X.509 94, 112, 120, 172, 250, 283
XKeyscore 306, 360

XML 361

XMPP 84, 255, 361

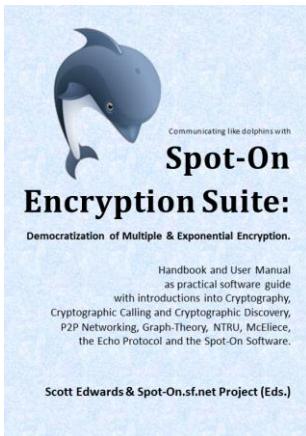
XOR 65, 66, 89, 324, 361

Y

YaCy 111, 362

Z

Zero-Knowledge 211, 213, 222, 301, 331, 363
Zero-Knowledge Proof 211, 222
Zero-Knowledge Protocol 363



Edwards, Scott &
Spot-On.sf.net Project (Eds.):

Communicating like dolphins with **Spot-On Encryption Suite:**

Democratization of Multiple & Exponential Encryption.

ISBN 9783749435067
BOD, Norderstedt 2019.

Spot-On Encryption Suite is a secure instant **chat** messenger and encrypting **e-mail** client that also includes additional features such as group chat, **file transfer**, and a **URL search** based on an implemented URL database, which can be peer-to-peer connected to other nodes. Also, further tools for file encryption or **text conversion to ciphertext** etc. are included.

The Spot-On program might currently be regarded as a very elaborated, up-to-date and diversified open source encryption software for **Multi-Encryption** and Cryptographic Calling: As it also includes the McEliece algorithm it is thus described as the **first McEliece Encryption Suite** worldwide – to be especially secure against attacks known from Quantum Computing.

Thus, the three basic functions frequently used by a regular Internet user in the **Internet** - communication (chat / e-mail), web search and file transfer - are now secure over the Internet within one software suite: **Open source** for everyone.

This handbook and user manual of Spot-On is a practical software guide with introductions not only to this application and its innovative and invented processes, but also into Encryption, Cryptography, **Cryptographic Calling** and **Cryptographic Discovery**, **Graph-Theory**, P2P Networking, NTRU, McEliece, the Echo Protocol and the Democratization of Multiple and **Exponential Encryption** also in the regard of the context of **Privacy** and **Human Rights**.

This "**Encyclopedia of modern Cryptography and Internet Security**" brings the latest and most relevant coverage of the topic - expanding a lot of relevant terms and central key words: *It's a Nomenclatura!*

- **Fundamental information** on modern Cryptography and Internet Security in a broadband overview.
- Extensive resource with most relevant explanations of keywords and terms.
- Introduction article by editing authors on "**Transformation of Cryptography**".
- Effective handbook **for students, tutors and researching professionals** in many fields and lecturing and developing experts of all levels to deepen the existing knowledge of the "**nomenclatura**" of these topics from Information Theory, Applied Mathematics, Technological Impact Assessment, for sure Linguistic, and Computational Methods of Engineering, Programming etc..
- Including the **didactic game for teaching**: "Cryptographic Cafeteria".
- With **bibliographic references** to start further readings.
- Appearing in an A-Z format, *Nomenclatura - The Encyclopedia of modern Cryptography and Internet Security* provides easy, intuitive access to scientific information on all relevant aspects of Cryptography, Encryption and Information and Internet Security.

This **modern Encyclopedia** is broad in scope, covering everything from AutoCrypt and Exponential Encryption to Zero-Knowledge-Proof Keys including explanations on Authentication, Block Ciphers and Stream Ciphers, Cryptanalysis and Security, Cryptographic Calling and Cryptographic Discovery, Cryptographic Protocols like e.g. the Echo-Protocol, Elliptic Curve Cryptography, Fiasco Forwarding, Goldbugs, Hash Functions and MACs, Juggling Juggernauts and Juggerknot Keys, McEliece, Multi-Encryption, NTRU, OTM, Public Key Cryptography, Patch-Points, POPTASTIC, Quantum Computing Cryptography, Secret Streams, Turtle Hopping, Two-Way-Calling and many more...

This introducing and cross-linking reference has been published in two popular formats: print and as eBook. The printed book edition has been created very affordable, so that each interested Reader, Researcher, Student and Tutor - and Library - is able to get this book with an investment comparable to a lunch meal to democratize **easy-accessible and readable** knowledge in one spot for **Cryptography, Encryption and Internet Security**.

