CRYPTOGRAPHIC TECHNOLOGY

RODEL URANI

Cryptography

- The practice and study of techniques for secure communication in the presence of third parties.
- Modern cryptography intersects the disciplines of and heavily based on mathematics theory, computer science practice, and electrical engineering.
    - Algorithms are designed around computational hardness assumptions.
    - Theoretically possible to break such system, invisible to do so any known practical means.
- Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

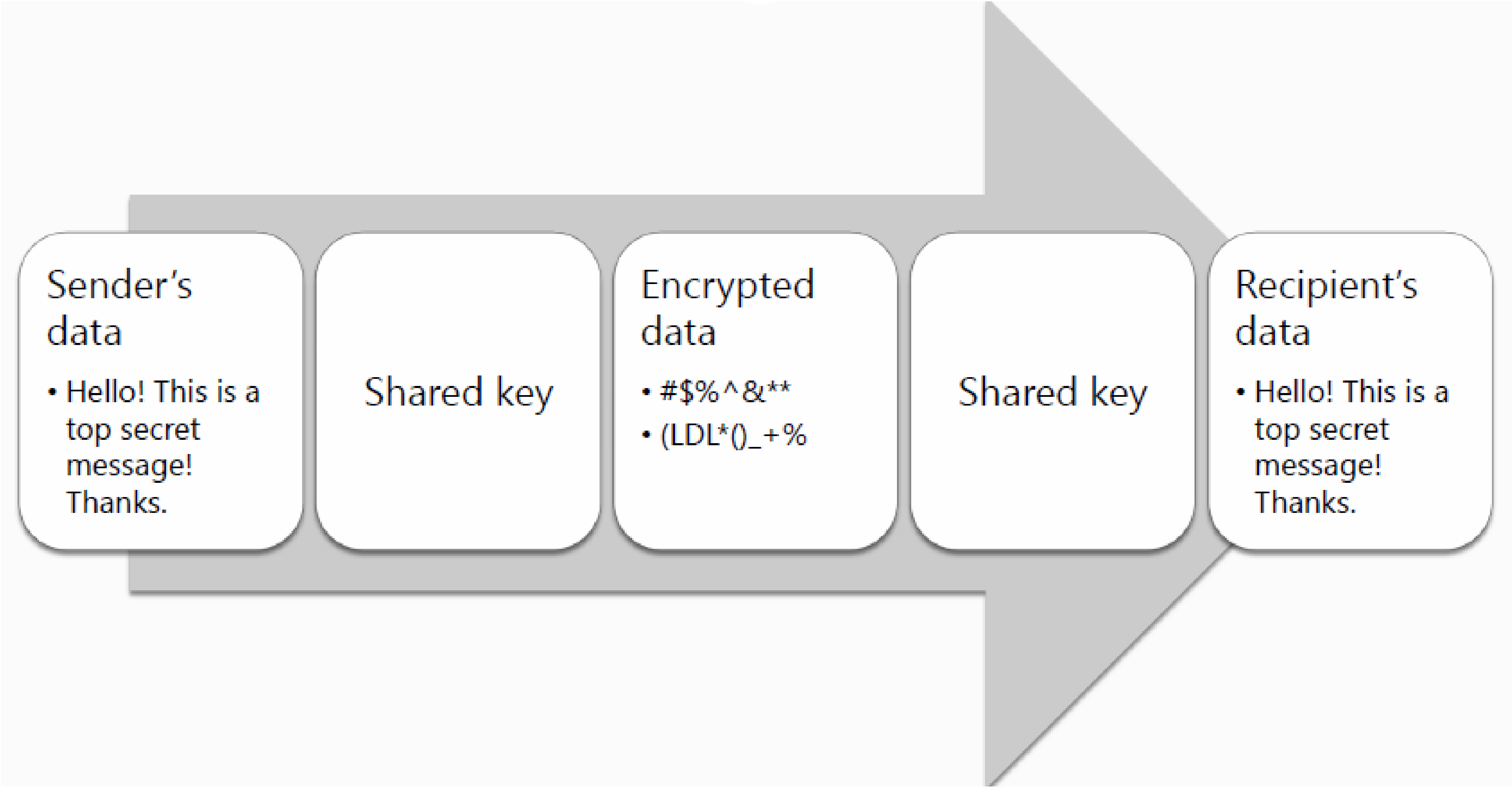
Central to modern cryptography

- Constructing and analyzing protocols that block adversaries.
- Various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation.
- Take note of the change of language from encryption (prior to modern age, present generation) to cryptography.

Crypto terms

- Encryption (until modern times), which is the process of converting ordinary information (called plaintext) into unintelligible text (called ciphertext).
- Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext.
- Cipher (or cypher) is a pair of algorithms that create the encryption and the reversing decryption.
- Cryptosystem is the ordered list of elements of finite possible plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption algorithms which correspond to each key.

What's in crypto, shared key?



Sender's data

- Hello! This is a top secret message! Thanks.

Shared key

Encrypted data

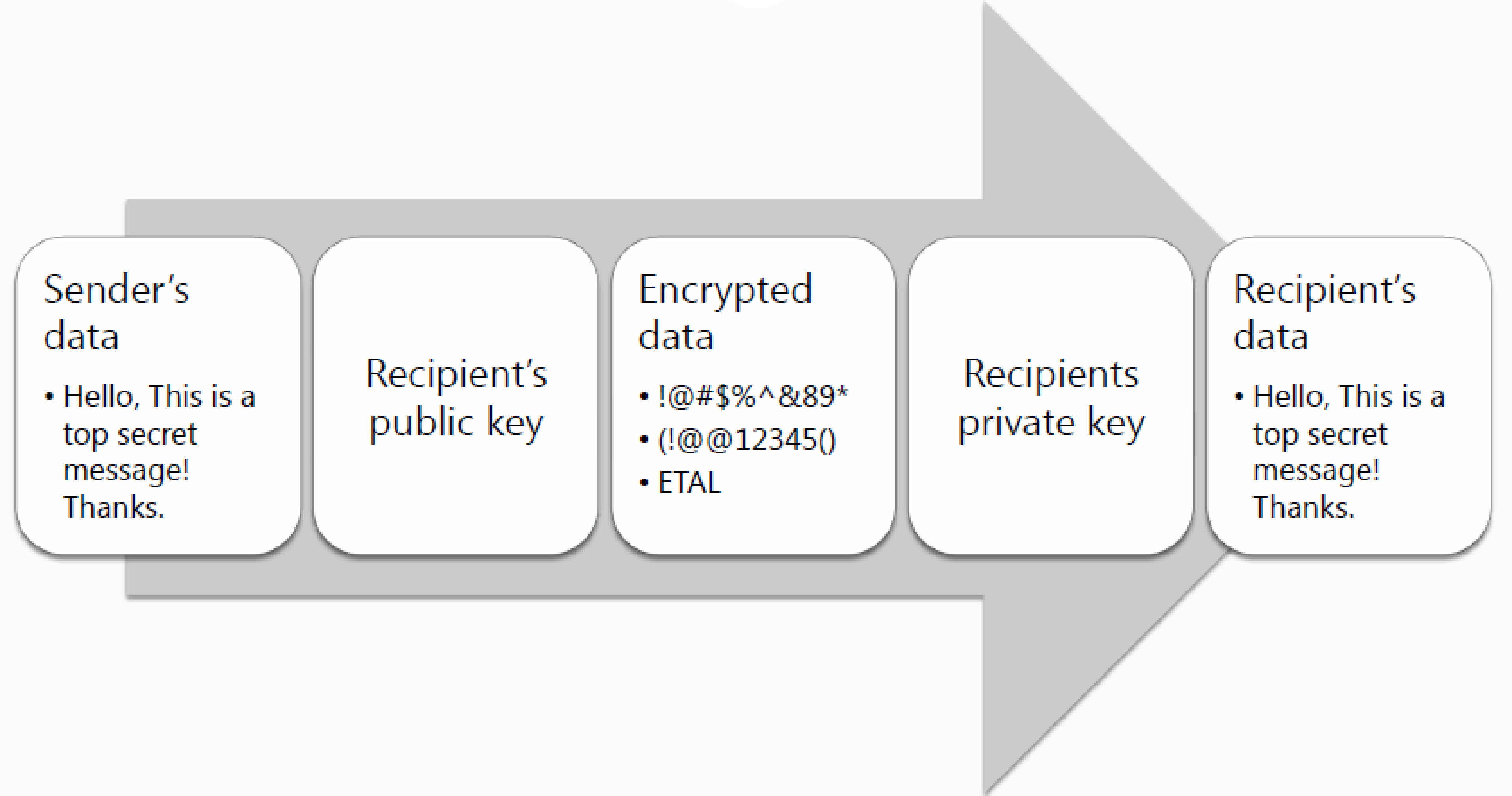
- #$%^&**
- (LDL*()_+%

Shared key

Recipient's data

- Hello! This is a top secret message! Thanks.

What’s in crypto, public key?



Sender’s data

- Hello, This is a top secret message! Thanks.

Recipient’s public key

Encrypted data

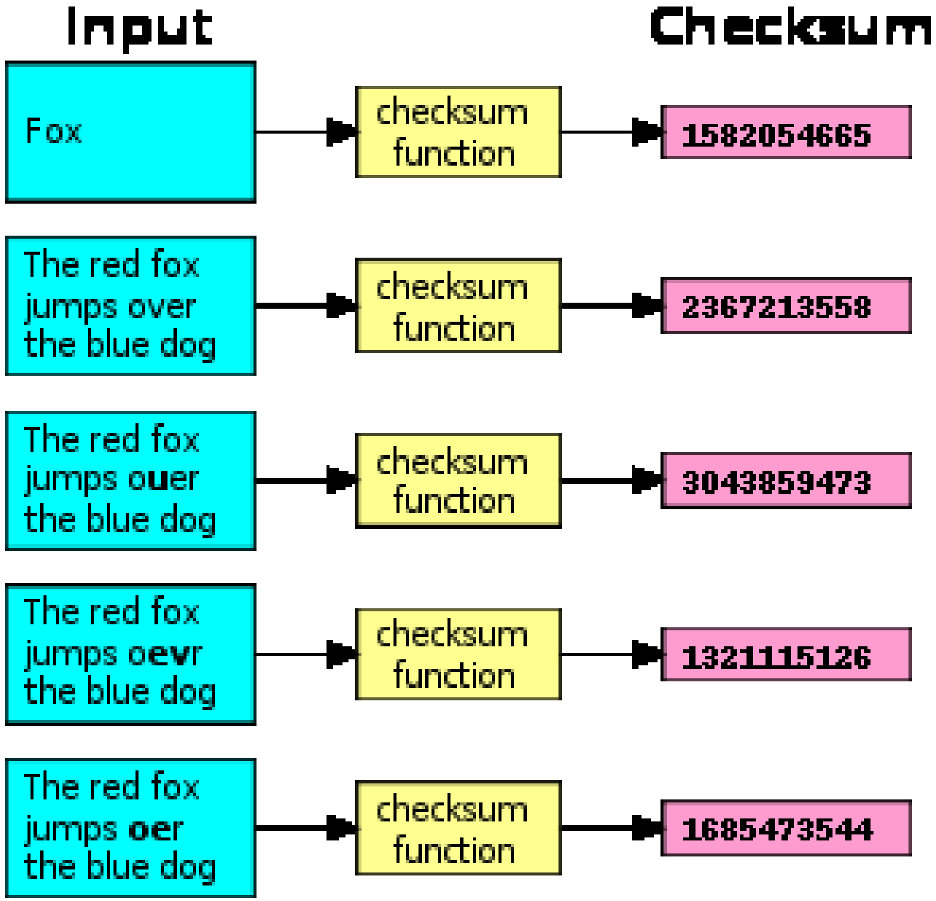
- !@#$%^&89*
- (!@@12345()
- ETAL

Recipients private key

Recipient’s data

- Hello, This is a top secret message! Thanks.

What's in crypto, checksum?



Cryptosystems or cryptographic protocols

- Symmertic
- Asymmetric
- Checksum/hashing

Symmetric key or shared key

- A method which both sender and receiver share the same key.
- Kind only known publicly until June 1976.
- Implemented as either block or stream ciphers.

Block ciphers

- Enciphers input in blocks of plaintext.
- Cipher designs and popular implementations
  - Data Encryption Standards (DES, withdrawn after AES adoption)
  - 3DES, variant of DES
  - Advance Encryption Standards
    - Designation cryptography standards by the U.S. government.

Block ciphers applications

- Security of data in
  - ATM
  - Email privacy
  - Remote access

Stream ciphers

- Enciphers individual characters.
- Creates an arbitrarily long stream of key material.
- Combined with the plaintext bit-by-bit or character-by-character.
- Cipher design and popular implementations
  - RC4 widely used
    - Speculations suggest may now be broken.

Stream cipher applications, RC4-based

- Transport Layer Security (TLS), used to protect Internet traffic.
  - Secure Sockets Layer, optional
- WEP
- WPA
- BitTorrent protocol encryption
- Microsoft Point-to-Point Encryption (MPPE)
- Secure Shell (SSH)
- Remote desktop i.e. Windows, *nix variants
- Kerberos, optional
- PDF
- Skype, modified form.
- Recommended replacement is Spritz.

Symmetric algorithms popular implementations

- Twofish
- Serpent
- AES
- Blowfish
- CAST5
- RC4
- Skipjack
- Safer+/++ (Bluetooth)
- IDEA

Symmetric key problems, susceptible to

- Known-plaintext attacks, an attack model for cryptanalysis where the attacker has samples of both the plaintext (called a **crib**), and its encrypted version (ciphertext).
- Chosen plaintext attacks, an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts.
- Differential cryptanalysis, a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions.
- Linear cryptanalysis, a general form of cryptanalysis based on finding affine approximations to the action of a cipher. Affine, see geometry about preserves points, straight lines and planes, sets of parallel lines, distances between points.

Asymmetric key or public key cryptosystem

- Constructed that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related.
- Private and public keys are generated secretly, as an interrelated pair.
- Public key may be freely distributed.
- Private key must remain secret.
- Based on the computational complexity of "hard" problems, often from number theory

Asymmetric key designs

- Involve operations such as modular multiplication and exponentiation, which are much more computationally expensive than the techniques used in most block ciphers, especially with typical key sizes.
- Diffie-Hellman key exchange protocol, now widely used in secure communications to allow two parties to secretly agree on a shared encryption key.
  - Sparked widespread academic efforts in finding a practical public-key encryption system.
- RSA algorithm, developed by Ronald Rivest, Adi Shamir, and Len Adleman.

Diffie–Hellman and RSA algorithms/cryptosystems

- Hardness
    - RSA is related to the integer factorization problem.
    - Diffie–Hellman and DSA are related to the discrete logarithm problem.
- First publicly known examples of high quality public-key algorithms.
- Have been among the most widely used.
- Other algorithms include
    - Cramer–Shoup cryptosystem,
    - ElGamal encryption, and various
    - Elliptic curve techniques.
    - Pretty Good Privacy (PGP).

Asymmetric key cryptosystems implementation

- Digital signature
- Transport Layer Security

Digital signature

- Is reminiscent of an ordinary signature; they both have the characteristic of being easy for a user to produce, but difficult for anyone else to forge.
- Be permanently tied to the content of the message being signed.
- Cannot be 'moved' from one document to another, for any attempt will be detectable.
- Central to the operations of public key infrastructures (PKI).

Transport Layer Security (TLS)

- And its predecessor, **Secure Sockets Layer** (**SSL**), are cryptographic protocols designed to provide communication security over a computer network.
- They use X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom they are communicating, and to exchange a symmetric key.

TLS applications

- Web browsing,
- Electronic mail,
- Internet faxing,
- Instant messaging, and
- Voice-over-IP (VoIP)

X.509

- An ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI).
- Specifies, amongst other things, standard formats for
  - Public key certificates,
  - Certificate revocation lists,
  - Attribute certificates, and a
  - Certification path validation algorithm.

X.509 consequence

- Both certificate authorities (CA) and a public key infrastructure (PKI) are necessary to verify the relation between a certificate and its owner, as well as to generate, sign, and administer the validity of certificates.

CA

- An entity that issues digital certificates.
- An organization that stores public keys and their owners, and every party in a communication trusts this organization (and knows its public key).
- 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 by the private key that corresponds to the certified public key.
- In this model of trust relationships, a CA is a trusted third party - trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.
- Accordingly, public-key infrastructure (PKI) schemes feature CAs.

CA security and legal applications

- Further the US E-Sign statute and the suggested UETA code help ensure that:
  - A signature, contract or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
  - A contract relating to such transaction may not be denied legal effect, validity or enforceability solely because an electronic signature or electronic record was used in its formation.
- Notaries are required in some cases to personally know the party whose signature is being notarized; this is a higher standard than is reached by many CAs.

CA market

- A W3Techs survey from December 2014 shows:
  - Symantec (which bought VeriSign's SSL interests and owns Thawte and Geotrust) with 35.7% market share
  - Comodo SSL with 26.9%
  - GlobalSign with 14.9%
  - Go Daddy with 13.0%
  - DigiCert with 3.4%
  - Entrust with 0.5%.

PKI

- A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
- An arrangement that binds public keys with respective user identities by means of a certificate authority (CA).
- A cryptographic technique that enables users to securely communicate on an insecure public network, and reliably verify the identity of a user via digital signatures.
- A system for the creation, storage, and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity.
- Creates digital certificates which map public keys to entities, securely stores these certificates in a central repository and revokes them if needed.

PKI consists of

- A certificate authority (CA) that both issues and verifies the digital certificates.
- A registration authority which verifies the identity of users requesting information from the CA.
- A central directory—i.e., a secure location in which to store and index keys.
- A certificate management system.
- A certificate policy.

Certification methods

- Certificate authorities (CAs),
- Web of trust (WoT), and
- Simple public key infrastructure (SPKI)

PKI use or utility

- Encryption and/or sender authentication of e-mail messages (e.g., using OpenPGP or S/MIME).
- Encryption and/or authentication of documents (e.g., the XML Signature or XML Encryption standards if documents are encoded as XML).
- Authentication of users to applications (e.g., smart card logon, client authentication with SSL). There's experimental usage for digitally signed HTTP authentication in the Enigform and mod_openpgp projects.
- Bootstrapping secure communication protocols, such as Internet key exchange (IKE) and SSL. In both of these, initial set-up of a secure channel (a "security association") uses asymmetric key—i.e., public key—methods, whereas actual communication uses faster symmetric key—i.e., secret key—methods.
- Mobile signatures are electronic signatures that are created using a mobile device and rely on signature or certification services in a location independent telecommunication environment.

Popular computer-based applications

- PGP wholedisk acquired by and now a Symantec company
- PGP email acquired by and now a Symantec company
- GNU Privacy Guard, open source
- Bitlocker (counterpart of PGP wholedisk) for Windows 7, earlier versions with Professional and Enterprise editions
- Encrypting File Systems

Crypto-related security technology

- Virtual Private Network (VPN)
- Authentication methods, check Kerberos
- WiFi Protected Access (WPA, WPA2)
- Internet services security provisioning i.e. Doman Name System Security (DNSSEC)

Virtual Private Network

- Internet Protocol Security (IPSecurity), open standard
- Used in establishment of Wide Area Network (WAN) especially for companies with presence in multiple locations.

IP Security (IPSec)

- A protocol suite, open standard, for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
- Includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.
- Can be used in protecting data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).
- Uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.
- An end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use operate in Application layer i.e. TLS and SSH.

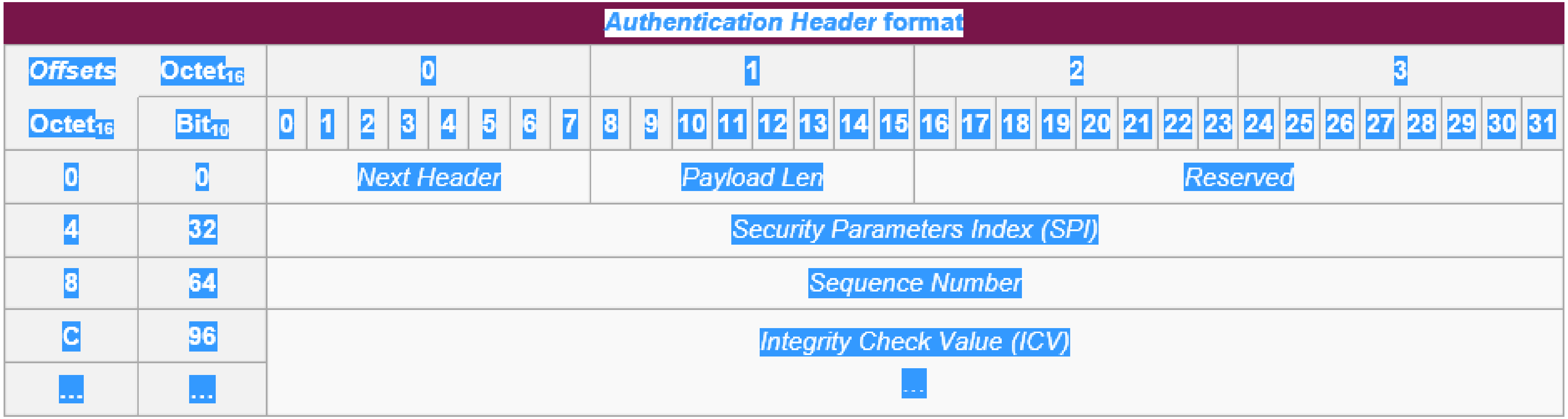
IPSec architecture

- Authentication Headers (AH)
- Encapsulating Security Payloads (ESP)
- Security Associations (SA)

IPSec architecture

- Authentication Headers (AH) provide connectionless integrity and data origin authentication for IP datagrams and provides protection against replay attacks.
- Encapsulating Security Payloads (ESP) provide confidentiality, data-origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic-flow confidentiality.
- Security Associations (SA) provide the bundle of algorithms and data that provide the parameters necessary for AH and/or ESP operations.
  - The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for authentication and key exchange, with actual authenticated keying material provided either by manual configuration with pre-shared keys, Internet Key Exchange (IKE and IKEv2), Kerberized Internet Negotiation of Keys (KINK), or IPSECKEY DNS records.

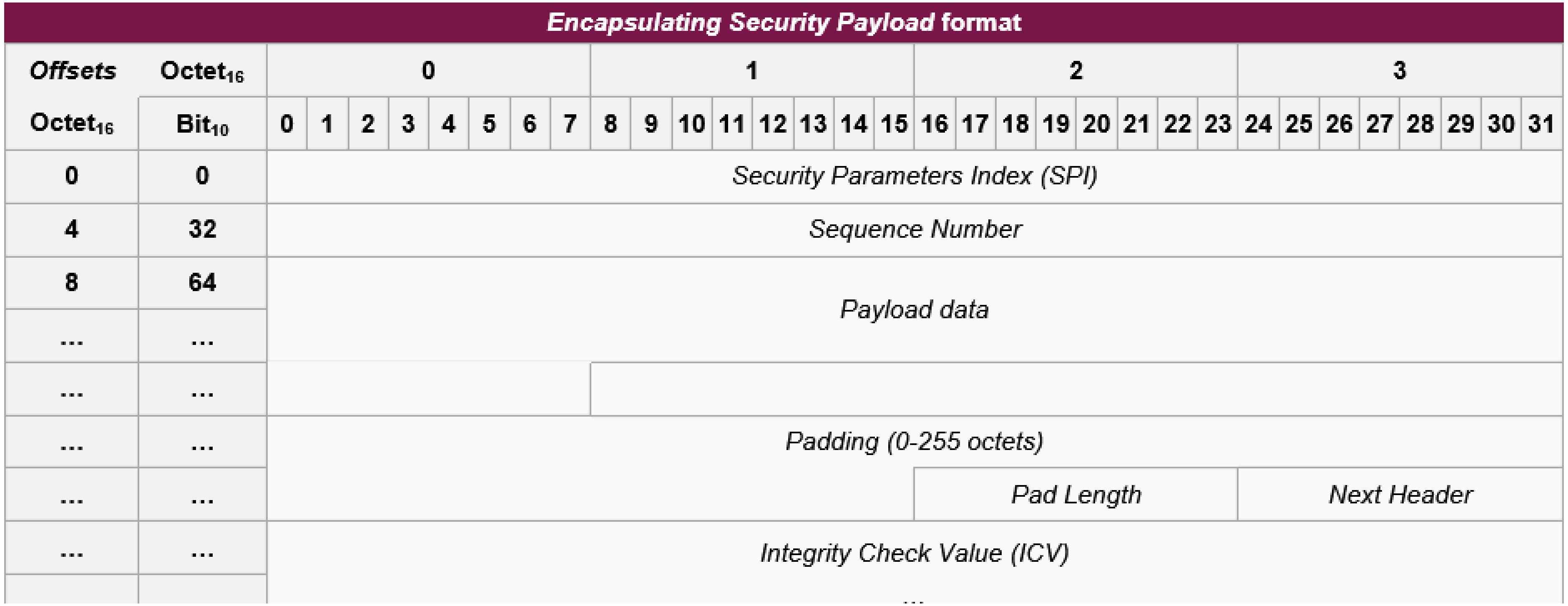
AH



Authentication Header format

Offsets	Octet$_{16}$	0								1								2								3							
Octet$_{16}$	Bit$_{10}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Next Header								Payload Len								Reserved															
4	32	Security Parameters Index (SPI)																															
8	64	Sequence Number																															
C	96	Integrity Check Value (ICV) …																															
…	…																																

ESP



***Encapsulating Security Payload* format**

Offsets	Octet$_{16}$	0								1								2								3							
Octet$_{16}$	Bit$_{10}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	*Security Parameters Index (SPI)*																															
4	32	*Sequence Number*																															
8	64	*Payload data*																															
...	...																																
...	...																																
...	...	*Padding (0-255 octets)*																															
...	...																	*Pad Length*								*Next Header*							
...	...	*Integrity Check Value (ICV)*																															
		...																															

IPSec modes of operation

- Transport mode
- Tunnel mode

IPSec transport mode

- The payload of the IP packet is usually encrypted and/or authenticated. The routing is intact, since the IP header is neither modified nor encrypted; however, when the authentication header is used, the IP addresses cannot be translated, as this will invalidate the hash value.
- The transport and application layers are always secured by hash, so they cannot be modified in any way (for example by translating the port numbers).
- A means to encapsulate IPsec messages for NAT traversal has been defined by RFC (Internet standard) documents describing the NAT-T mechanism.

IPSec tunnel mode

- The entire IP packet is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access) and host-to-host communications (e.g. private chat).
- Tunnel mode supports NAT traversal.

IPSec cryptographic algorithms

- HMAC-SHA1 for integrity protection and authenticity.
- TripleDES-CBC for confidentiality
- AES-CBC for confidentiality.
- AES-GCM providing confidentiality and authentication together efficiently.

- Refer to RFC 7321 for details.

Authentication methods, Kerberos

- A computer network authentication protocol which 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.
- Designed to provide strong authentication for client/server applications by using secret-key cryptography.
- Builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication.
- Uses **strong cryptography** so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.
- Uses UDP port 88 by default.

Kerberos on platforms' implementations

- MS Windows Server 2000
- Unix/Linux variants
  - FreeBSD,
  - Apple's Mac OS X,
  - Red Hat Enterprise Linux,
  - Oracle's Solaris,
  - IBM's AIX and Z/OS,
  - HP's OpenVMS.

Internet services security provisioning, DNSSEC

- A suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.

Computer networks and Internet routing, RPKI

- Known as Resource Certification, is a specialized public key infrastructure (PKI) framework designed to secure the Internet's routing infrastructure.
- RPKI provides a way to connect Internet number resource information (such as Autonomous System numbers and IP addresses) to a trust anchor. The certificate structure mirrors the way in which Internet number resources are distributed.
- Resources are initially distributed by the IANA to the Regional Internet Registries (RIRs), who in turn distribute them to Local Internet registries (LIRs), who then distribute the resources to their customers.
- Can be used by the legitimate holders of the resources to control the operation of Internet routing protocols to prevent route hijacking and other attacks.
- Used to secure the Border Gateway Protocol (BGP) through BGPSEC, as well as Neighbor Discovery Protocol (ND) for IPv6 through the Secure Neighbor Discovery Protocol (SEND).

Neighbor Discovery Protocol

- A protocol in the Internet protocol suite used with Internet Protocol Version 6 (IPv6).
- It operates in the Link Layer of the Internet model (RFC 1122) and is responsible for address autoconfiguration of nodes, discovery of other nodes on the link, determining the link layer addresses of other nodes, duplicate address detection, finding available routers and Domain Name System (DNS) servers, address prefix discovery, and maintaining reachability information about the paths to other active neighbor nodes (RFC 4861).

Secure Neighbor Discovery

- Uses Cryptographically Generated Addresses (CGA) and other new NDP options for the ICMPv6 packet types used in NDP.
- CGA is an Internet Protocol Version 6 (IPv6) address that has a host identifier computed from a cryptographic hash function. This procedure is a method for binding a public signature key to an IPv6 address here, see SEND further.

Cryptography standards, PKCS #1-15

- #1 RSA Cryptography Standard. See RFC 3447. Defines the mathematical properties and format of RSA public and private keys (ASN.1-encoded in clear-text), and the basic algorithms and encoding/padding schemes for performing RSA encryption, decryption, and producing and verifying signatures.
- #3 Diffie–Hellman Key Agreement Standard. A cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
- #5 Password-based Encryption Standard. See RFC 2898 and PBKDF2.
- #6 Extended-Certificate Syntax Standard. Defines extensions to the old v1 X.509 certificate specification. Obsoleted by v3 of the same.
- #7 Cryptographic Message Syntax Standard. See RFC 2315. Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination (for instance as a response to a PKCS#10 message). Formed the basis for S/MIME, which is as of 2010 based on RFC 5652, an updated Cryptographic Message Syntax Standard (CMS). Often used for single sign-on.
- There is more at http://en.wikipedia.org/wiki/PKCS

Crypto regulated as weapon*

- U.S.
- Canada

Cryptlib security principles

- Security architecture properties
- Security architecture design goals
- Kernel controls and policies

Security architecture properties

- Permission-based access, the default access/use permission should be deny-all, with access or usage rights being made selectively available as required.
- Least privilege and isolation, each object should operate with the least privileges possible to minimize damage due to inadvertent or deliberate compromise of the information or capabilities they contain.
- Complete mediation, each object access is checked each time that the object is used.
- Economy of mechanism and open design, the protection system design should be as simple as possible in order to allow it to be easily checked, tested and trusted and should not rely on security through obscurity.
- Easy to use, in order to promote its use, the projection system should be as easy to use and transparent as possible to the user.

Security architecture design goals

- Separation of policy and mechanism, the policy component deals with context-specific decisions about objects and requires detailed knowledge abou thte semantics of each object type.
- Verifiable design, should be possible to apply formal verification techniques to the security-critical portion of the architecture (the security kernel) in order to provide a high degree of confidence that the security measures are implemented as intended.
- Flexible security policy, was hardcoded into the implementation. Since not all users require the same policy, it should be relatively easy to adapt policy details to user specific requirements.
- Efficient implementation, the 1980s was an abysmal performance. Security kernel, therefore, should provide high level performance to the extent that the user isn't even aware of the presence of the kernel.
- Simplicity, making the possibility to implement an extremely simple, efficient, and easy-to-verify kernel design.

Kernel controls and policies

- Separation, objects are isolated and can communicate only via kernel. Benefit: Simplified implementation and the ability to use a special-purpose kernel that is very amenable to verification.
- No ability to run user code, users just supply data to be acted upon by the objects. Benefit: Vastly simplified implementation and verification.
- Single-level object security, no information sharing. Benefit: Simplified implementation and verification.
- Serialization of operations with objects, ensuring certain operations are performed in the correct sequence. Benefit: Kernel-mandated control over how objects are used.
- Object usage controls, whether an object can be used for a particular purpose and the number of times the object can be used before access is disabled. Benefit: Precise user control over the object rather than an uncontrolled number of signatures under a trojan horse.

Cryptlib applications

- Elliptic Curve Cryptography
- S/MIME
- CA Operations
- SSH, SSL & TLS
- PGP/OPENPGP
- PKI Services

Elliptic Curve Cryptography

- An approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The US National Security Agency has endorsed it by including schemes based on ECC in its ‘Suite B’ set of recommended algorithms and allows their use for protecting information classified up to Top Secret. cryptlib’s implementation of ECC meets the requirements for NSA Suite B use.

S/MIME

- Employs the IETF-standardised Cryptographic Message Syntax (CMS, formerly called PKCS #7) format as its native data format. CMS is the underlying format used in the **S/MIME** secure mail standard, as well as a number of other standards covering secure EDI and related systems like HL7 medical messaging and the Session Initiation Protocol (SIP) for services like Internet telephony and instant messaging.

CA Operations

- A scalable, flexible **engine (CA)** built on the transaction-processing capabilities of a number of proven, industrial-strength relational databases running on a variety of hardware platforms. The CA facility provides an automated means of handling certificate issuance without dealing directly with the details of processing request, signing certificates, saving the resulting certificates in keys stores, and assembling CRLs. This constitutes a complete CA system for issuance and management of certificates and CRLs.

SSH, SSL & TLS

- Takes care of the session details for you so that all you need to do is provide basic communications information such as the name of the server or host to connect to and any other information required for the session such as a password or certificate. cryptlib takes care of establishing the session and managing the details of the communications channel and its security parameters, and provides both client and server implementations of all of these session types.

PGP/OPENPGP

- Message format alongside the PKCS #7/CMS/SMIME formats, allowing it to be used to send and receive PGP-encrypted email and data. As with the S/MIME implementation, the **PGP implementation** uses cryptlib's enveloping interface to allow simple, rapid integration of strong encryption and authentication capabilities into existing email agents and messaging software.
- Since the enveloping interface is universal, the process involved in creating **PGP** and **S/MIME messages** is identical except for the envelope format specifier, allowing a one-off development effort to handle any secure message format.

PKI Services

- Implements full range i.e. (PKI services, aside from SSH, SSL and TLS) in its secure session interface, again providing both client and server implementations of all protocols.
- These services include the
  - Certificate management protocol (CMP),
  - Simple certificate enrolment protocol (SCEP),
  - Real-time certificate status protocol (RTCS),
  - Online certificate status protocol (OCSP), and
  - Timestamping (TSP).

Certificate management protocol (CMP)

Simple certificate enrolment protocol (SCEP)

Real-time certificate status protocol (RTCS)

Online certificate status protocol (OCSP)

Timestamping (TSP)

Integrate crypto in apps?

- No shortcut, accordingly it is a distinct field.
- Refer to
  - Cryptographic engineering
  - Security engineering.