菩萨相谈

菩

Wfujqhlagf

Ozq Al Esllwjk

Brian Sletten (@bsletten)

02/17/2016

Encryption

Why It Matters

Brian Sletten (@bsletten)

02/17/2016

Speaker Qualifications

- Specialize in next-generation technologies
- Author of O'Reilly Videos on Hypermedia and Linking Data
- Author of 'Resource-Oriented Architecture Patterns for Webs of Data'
- Teaches and speaks internationally about REST, Semantic Web, Data Science, Security, Visualization, Architecture
- Worked in Defense, Finance, Retail, Hospitality, Video Game, Health Care, Telecommunications and Publishing Industries
- International Pop Recording Artist

Agenda

- Ciphers
- Symmetric Encryption
- Asymmetric Encryption
- The World We Live In

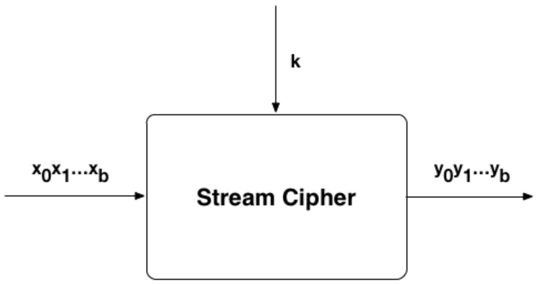
Ciphers

One-Time Pad

- Information-theoretically secure
- Ciphertext is created by combining input with a shared random key
- Perfect secrecy
- Immune to brute-force attacks
- Requires perfectly random keys
- Keys cannot be reused ever
- Keys have to be as long as the input

XOR

A	B	Output
0	0	0
0	1	1
1	0	1
1	1	0



k

$x_0x_1 \ldots x_b$

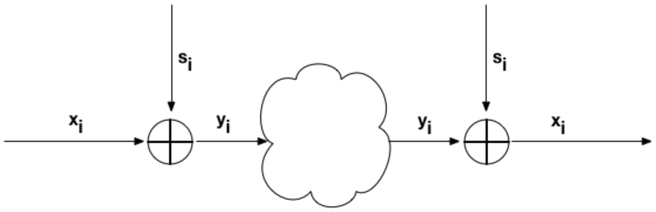
Stream Cipher

$y_0y_1 \ldots y_b$

Credit: Understanding Cryptography: A Textbook for Students and Practitioners

$$y_i = e_{si}\left(x_i\right) \equiv x_i + s_i \, mod \, 2$$

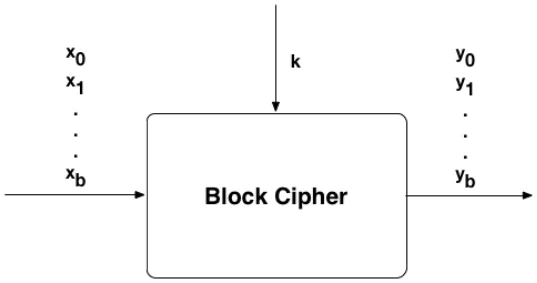
Credit: Understanding Cryptography: A Textbook for Students and Practitioners



Credit: Understanding Cryptography: A Textbook for Students and Practitioners

Stream Ciphers

- Encryption and Decryption are the same
- Modulo 2 addition is equivalent to XOR
- Security of the system is based upon keystream



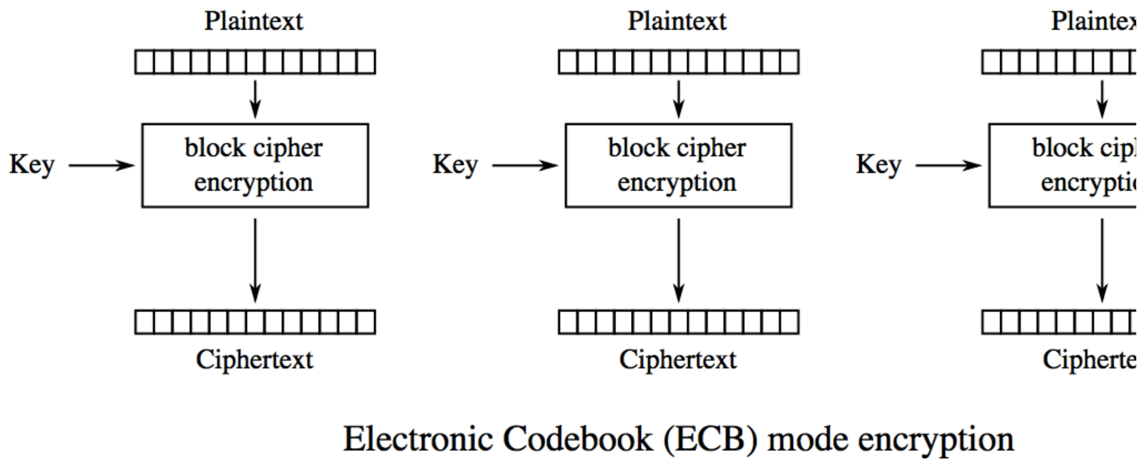
Credit: Understanding Cryptography: A Textbook for Students and Practitioners

Block Cipher Modes

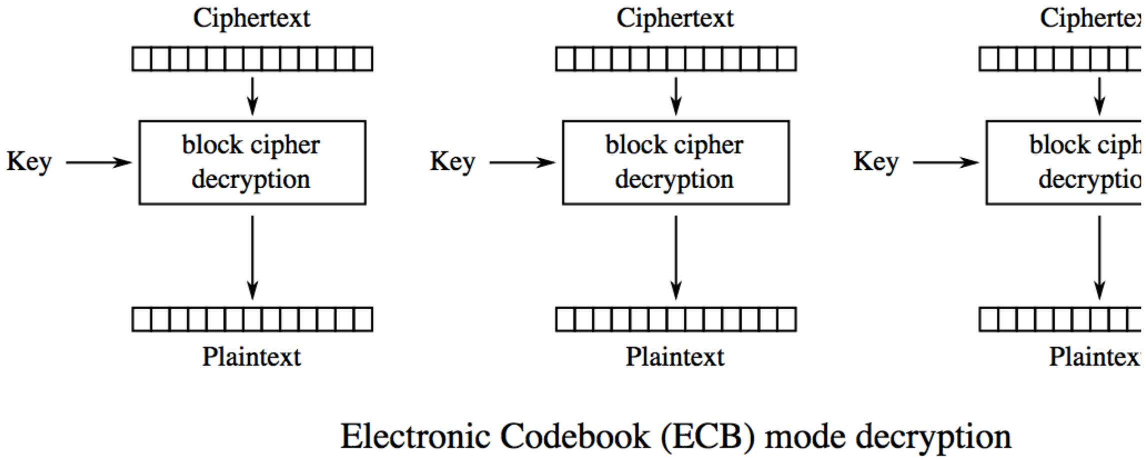
- Electronic Cookbook (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFB)
- Counter Mode (CTR)
- Galois Counter Mode (GCM)

Electronic Cookbook (ECB)

- Every block (num bits of size) is independently encrypted and decrypted
- Blocks of < num bits are padded
- Parallelizable
- Errors only affect individual blocks



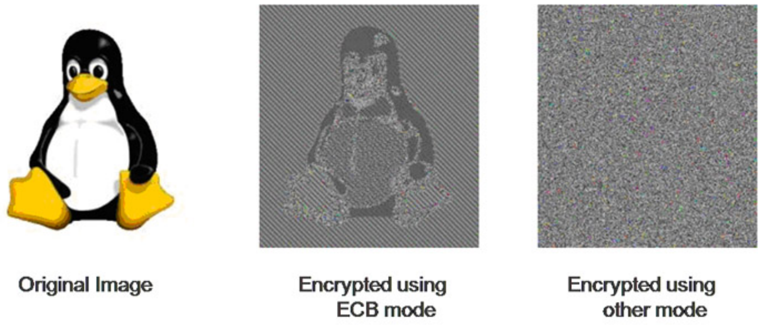
Credit: Wikipedia



Credit: Wikipedia

Problems With ECB

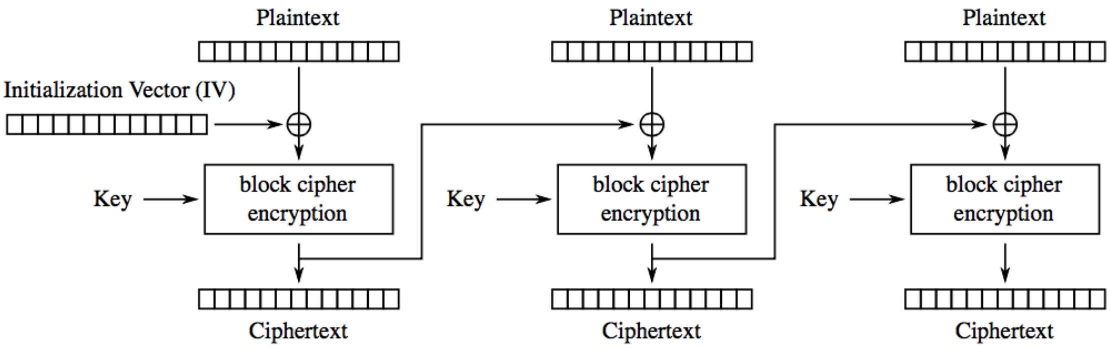
- Block reordering cannot be detected
- Block substitutions are possible
- Highly deterministic



Credit: Kingston

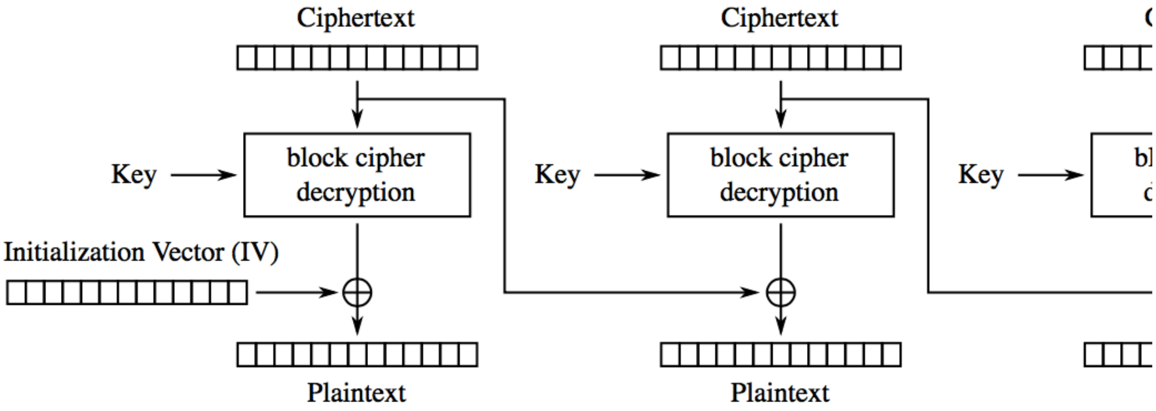
Cipher Block Chaining (CBC)

- Use of Initialization Vector (IV) reduces determinism
- Output of each block is XORed with next block and then encrypted
- Messages are still modifiable, but not deterministically



Cipher Block Chaining (CBC) mode encryption

Credit: Wikipedia

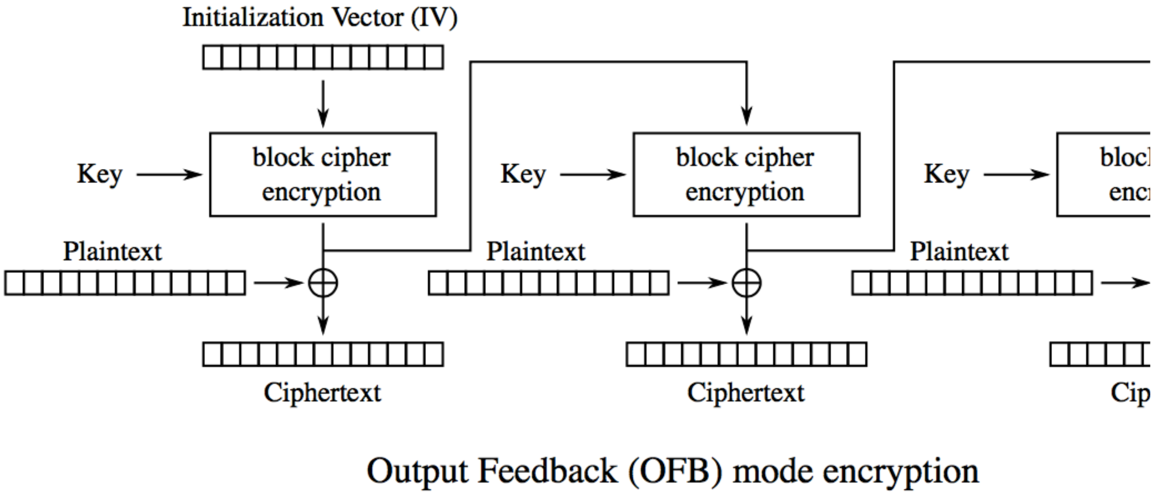


Cipher Block Chaining (CBC) mode decryption

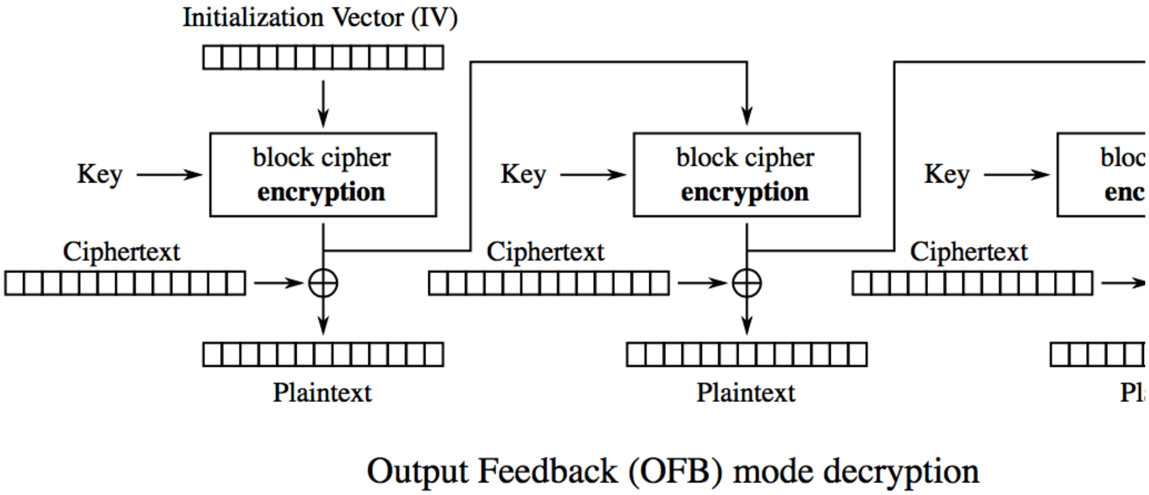
Credit: Wikipedia

Output Feedback Mode (OFB)

- Block cipher is used to create a stream cipher
- Stream is computed as blocks, not bits
- Encrypt an IV to generate num bits
- Next num bits is generated by encrypting the output of previous block
- Key stream can be pre-computed
- Encryption and Decryption are the same



Credit: Wikipedia



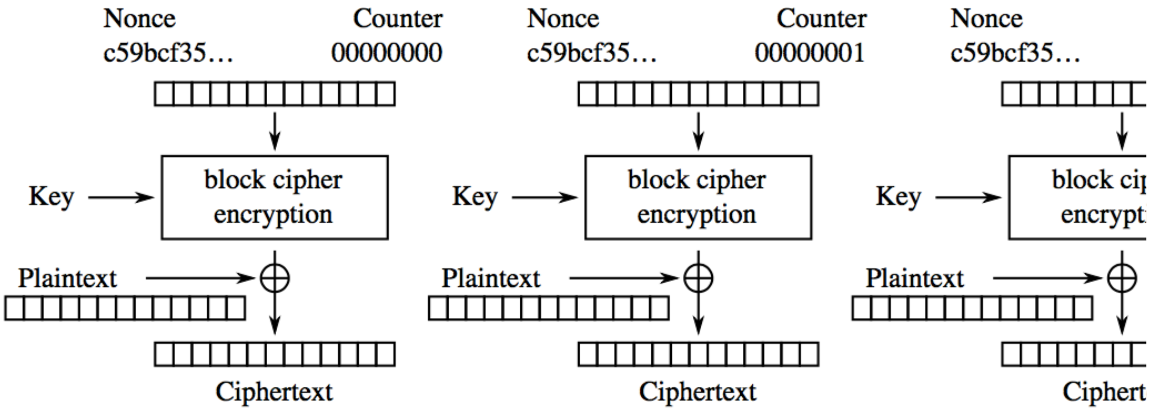
Credit: Wikipedia

Cipher Feedback Mode (CFB)

- Similar to OFB but ciphertext is fed back into keystream generation
- Can be basis for handling short, bursty traffic of blocks < num bits

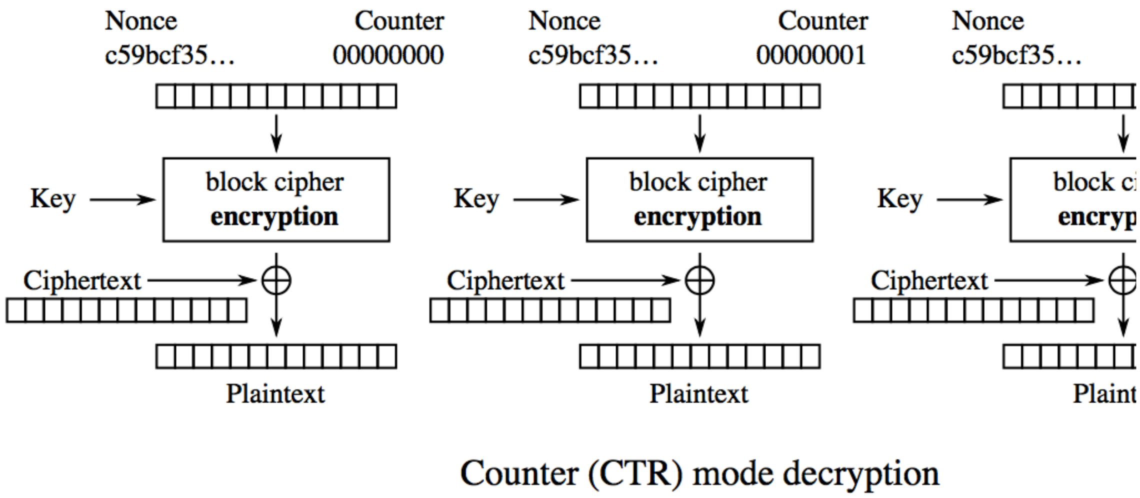
Counter Mode (CTR)

- Also uses block cipher to generate keystream
- IV is chosen to be less than block size
- Remaining bits are used as a counter
- Does not require feedback chaining so can be parallelized for improved performance



Counter (CTR) mode encryption

Credit: Wikipedia



Credit: Wikipedia

Hash Functions

- Generate a fixed-size output from arbitrary input
- Computationally unfeasible to reverse a hash
- Computationally unfeasible to generate a message for a given hash
- Computationally unfeasible to find two inputs that generate the same hash

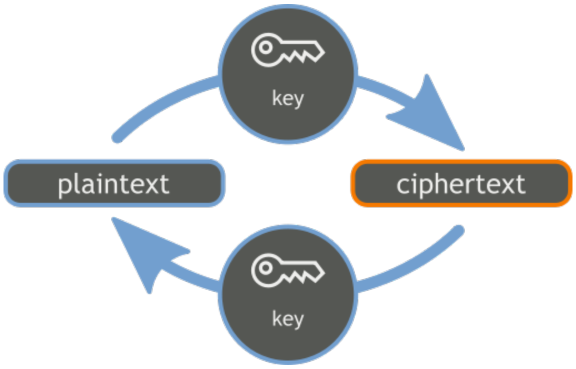
Message Authentication Code (MAC)

- Verify data integrity and authenticity
- Cannot be sent with data itself
- Hashing key must be shared

Galois Counter Mode (GCM)

- Combines Counter Mode with Galois authentication
- Authenticity and Confidentiality
- MAC is generated
- Parallelizable

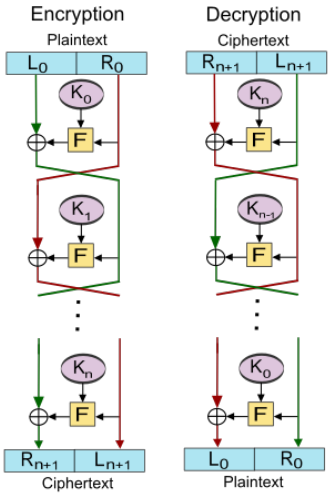
Symmetric Encryption



Credit: Bananenfalter

Data Encryption Standard (DES)

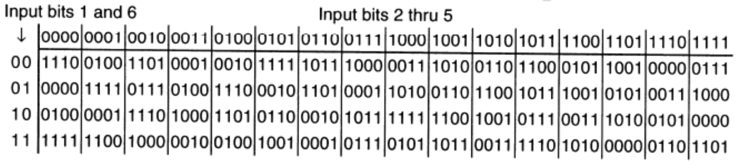
- NBS (with NSA consultation) requested proposals for ciphers to be used for unclassified but sensitive purposes
- Lucifer cipher from IBM based upon Feistel networks



Credit: Wikipedia

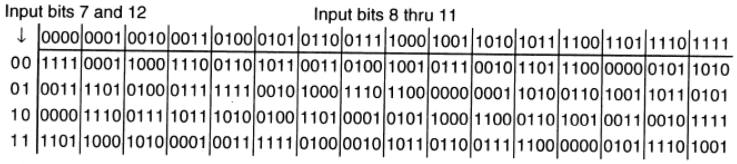
Data Encryption Standard (DES)

- Convinced IBM to reduce keysize to 56 bits
- Changed the definition of the 'S-Boxes'
- Claim no involvement in the algorithm design



Input bits 1 and 6	Input bits 2 thru 5															
↓	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

Figure 3-9. Table of 4-bit outputs of S-box 1 (bits 1 thru 4)



Input bits 7 and 12	Input bits 8 thru 11															
↓	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1111	0001	1000	1110	0110	1011	0011	0100	1001	0111	0010	1101	1100	0000	0101	1010
01	0011	1101	0100	0111	1111	0010	1000	1110	1100	0000	0001	1010	0110	1001	1011	0101
10	0000	1110	0111	1011	1010	0100	1101	0001	0101	1000	1100	0110	1001	0011	0010	1111
11	1101	1000	1010	0001	0011	1111	0100	0010	1011	0110	0111	1100	0000	0101	1110	1001

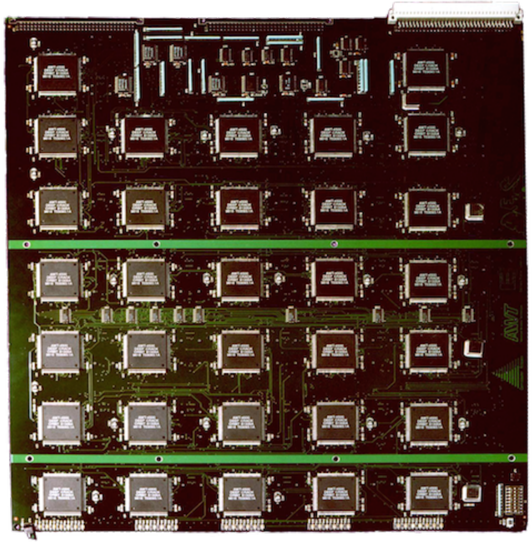
Figure 3-10. Table of 4-bit outputs of S-box 2 (bits 5 thru 8)

> “In 1973 NBS solicited private industry for a data encryption standard (DES). The first offerings were disappointing, so NSA began working on its own algorithm. Then Howard Rosenblum, deputy director for research and engineering, discovered that Walter Tuchman of IBM was working on a modification to Lucifer for general use. NSA gave Tuchman a clearance and brought him in to work jointly with the Agency on his Lucifer modification.”

Thomas R. Johnson
American Cryptology during the Cold War, 1945-1989.Book III: Retrenchment and Reform, 1972-1980

Differential Cryptanalysis (DC)

- An attack on block ciphers, stream ciphers and hashing functions
- How do changes in the input affect the output
- Discovered in the 1980s by Eli Biham and Adi Shamir
- Proposed a potential weakness in DES
- 1994 DES team published a paper claiming knowledge of DC since 1974 and that they designed against it



Triple Data Encryption Standard (3DES)

- Extend the life of the cipher while gaining protection
- Three independent keys are used for a key length of 168 bits
- MITM attack limits the strength to effective keylength of 112 bits
- SLOW

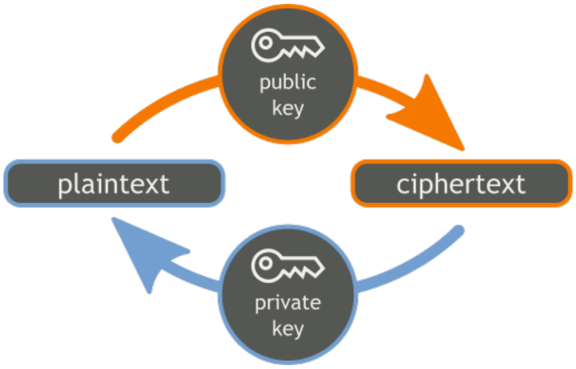
Advanced Encryption Standard (AES)

- Developed by NIST between 1997 and 2000
- Open process requesting designs
- CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, Rijndael, SAFER+, Serpent, and Twofish
- Wanted reasonable performance in a variety of environments
- Rijndael was chosen in 2000
- FIPS Pub 197 accepted in 2001
- Well-received by the crypto community

Advanced Encryption Standard (AES)

- Not based on Feistel networks
- Supports key sizes of 128, 192 and 256 bits
- Between 10-14 rounds
- SubBytes, ShiftRows, MixColumns, AddRoundKey
- Mostly side channel attacks although some better than brute force (but still hard) have been discovered
- Government has approved it for up to TS

Asymmetric Encryption



Credit: Bananenfalter

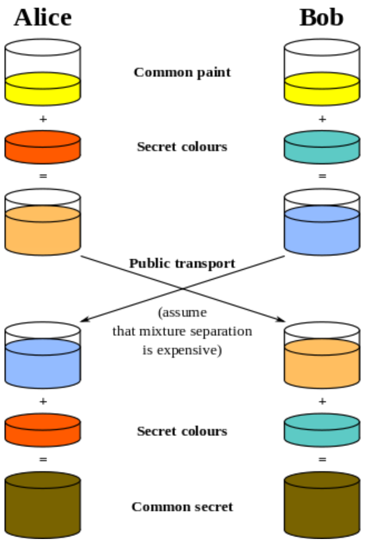
Diffie-Helman Key Exchange (DHKE)

- First published asymmetric crypto scheme (1976)
- Influenced by work of Ralph Merkle
- Discovered earlier at GCHQ but was classified
- Allows derivation of a secret key over public channels
- Based upon the Discrete Logarithm Problem

$$\alpha^x \equiv \beta \, mod \, p$$

$$x = log_{\alpha}\beta \, mod \, p$$

$$k = (\alpha^{x})^{y} \equiv (\alpha^{y})^{x} \; mod \, p$$

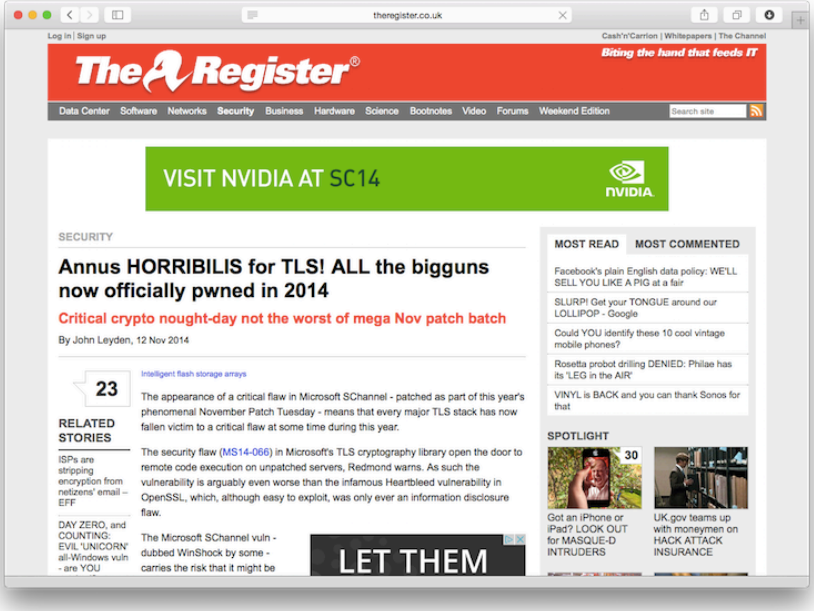


Credit: Wikipedia

DHKE Uses

- SSH
- TLS
- IPSec

The World We Live In



SECURITY

Annus HORRIBILIS for TLS! ALL the bigguns now officially pwned in 2014

Critical crypto nought-day not the worst of mega Nov patch batch

By John Leyden, 12 Nov 2014

23

RELATED STORIES

ISPs are stripping encryption from netizens' email – EFF

DAY ZERO, and COUNTING: EVIL 'UNICORN' all-Windows vuln - are YOU

Intelligent flash storage arrays

The appearance of a critical flaw in Microsoft SChannel - patched as part of this year's phenomenal November Patch Tuesday - means that every major TLS stack has now fallen victim to a critical flaw at some time during this year.

The security flaw (MS14-066) in Microsoft's TLS cryptography library open the door to remote code execution on unpatched servers, Redmond warns. As such the vulnerability is arguably even worse than the infamous Heartbleed vulnerability in OpenSSL, which, although easy to exploit, was only ever an information disclosure flaw.

The Microsoft SChannel vuln - dubbed WinShock by some - carries the risk that it might be

Facebook's plain English data policy: WE'LL SELL YOU LIKE A PIG at a fair

SLURP! Get your TONGUE around our LOLLIPOP - Google

Could YOU identify these 10 cool vintage mobile phones?

Rosetta probot drilling DENIED: Philae has its 'LEG in the AIR'

VINYL is BACK and you can thank Sonos for that

Got an iPhone or iPad? LOOK OUT for MASQUE-D INTRUDERS

UK.gov teams up with moneymen on HACK ATTACK INSURANCE

Failures in Implementations

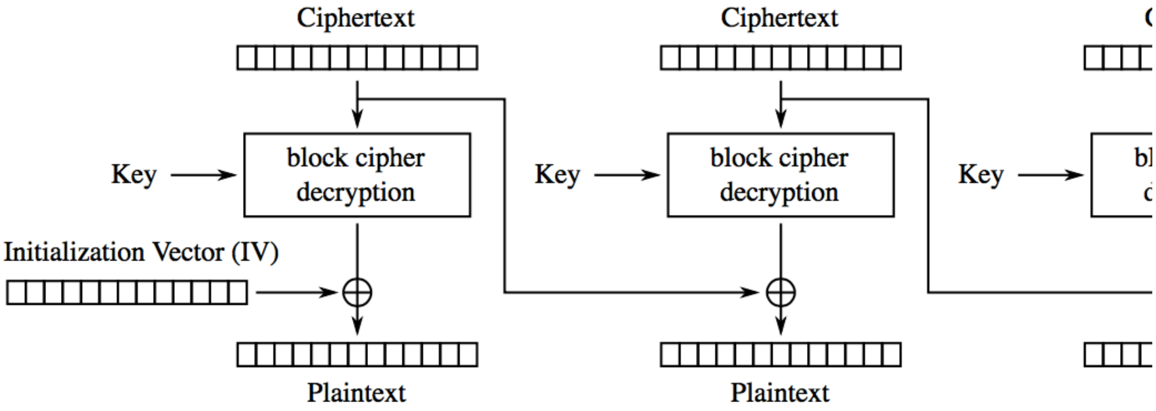
- Apple SecureTransport - 'Triple Handshake'
- GNUTLS - Bad Cert Validation/MITM
- OpenSSL - Heartbleed
- NSS - Signature Forgery Flaw (ASN.1 parsing)
- Microsoft SChannel

Known TLS Hacks

- BEAST
- CRIME
- BREACH
- Lucky Thirteen
- POODLE

Padding Oracle on Downgraded Legacy Encryption (POODLE)

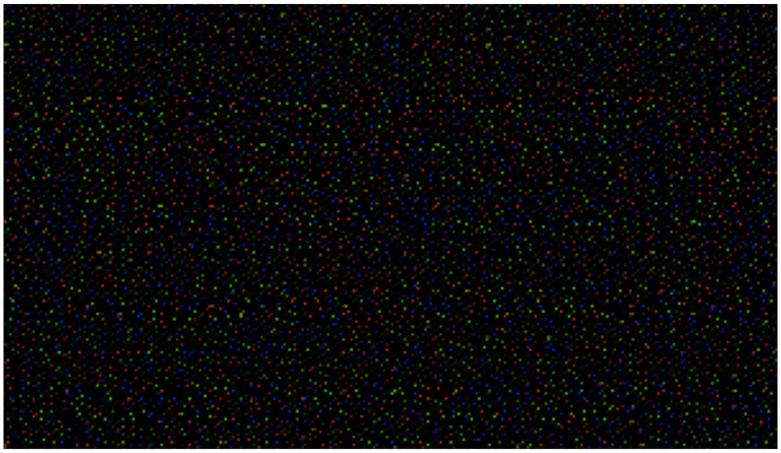
- Simulate a failure during negotiation
- Downgrade browser and server to SSL3
- Problem is in the protocol, not an implementation
- Must disable SSL3 in browser and server



Cipher Block Chaining (CBC) mode decryption

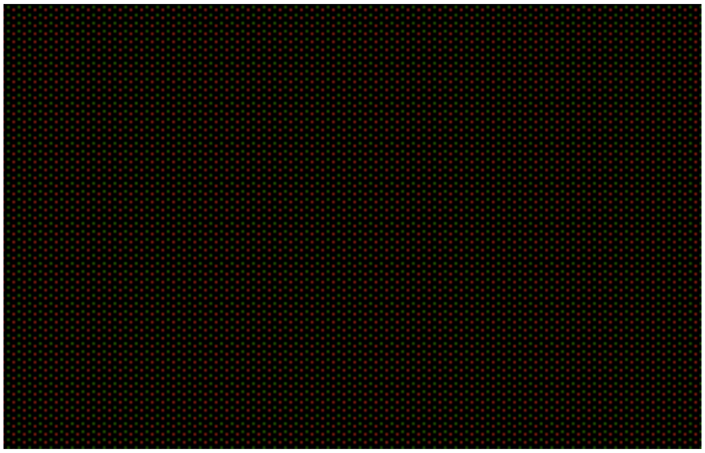
Credit: Wikipedia

AES Timing Variability

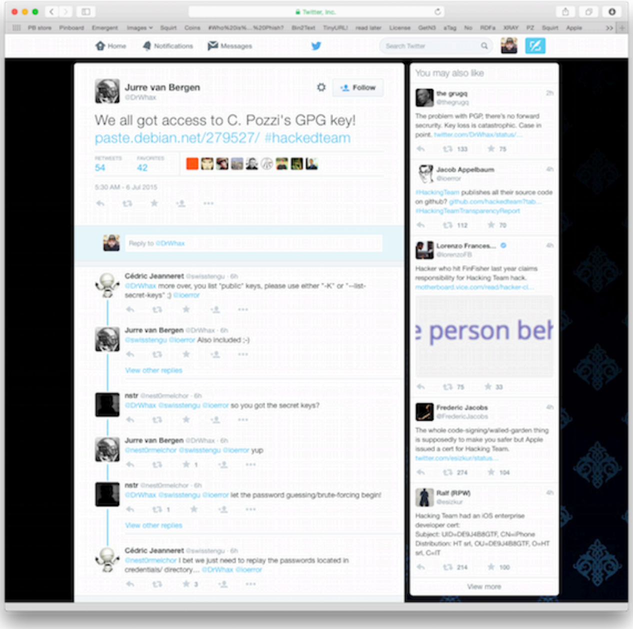


Credit: http://cr.yp.to

More Constant Time AES w/ Caching



Credit: http://cr.yp.to


Twitter, Inc.
Pinboard Emergent Images Squirt Coins #Who%20is%...%20Phish? Bin2Text TinyURL! read later License GetN3 aTag No RDFa XRAY PZ Squirt Apple
Home
Notifications
Messages
Search Twitter
Follow
Reply to @DrWhax
You may also like
View more

Jurre van Bergen @DrWhax

We all got access to C. Pozzi's GPG key! paste.debian.net/279527/ #hackedteam

RETWEETS 54 FAVORITES 42

5:30 AM - 6 Jul 2015

Cédric Jeanneret @swisstengu · 6h
@DrWhax more over, you list "public" keys, please use either "-K" or "--list-secret-keys" ;) @ioerror

Jurre van Bergen @DrWhax · 6h
@swisstengu @ioerror Also included ;-)

View other replies

nstr @nest0rmelchor · 6h
@DrWhax @swisstengu @ioerror so you got the secret keys?

Jurre van Bergen @DrWhax · 6h
@nest0rmelchor @swisstengu @ioerror yup

★ 1

nstr @nest0rmelchor · 6h
@DrWhax @swisstengu @ioerror let the password guessing/brute-forcing begin!

1

View other replies

Cédric Jeanneret @swisstengu · 6h
@nest0rmelchor I bet we just need to replay the passwords located in credentials/ directory.... @DrWhax @ioerror

★ 3

the grugq @thegrugq 2h
The problem with PGP, there's no forward secrurity. Key loss is catastrophic. Case in point. twitter.com/DrWhax/status/...
133 ★ 75

Jacob Appelbaum @ioerror 4h
#HackingTeam publishes all their source code on github? github.com/hackedteam?tab... #HackingTeamTransparencyReport
112 ★ 70

Lorenzo Frances... @lorenzoFB 4h
Hacker who hit FinFisher last year claims responsibility for Hacking Team hack. motherboard.vice.com/read/hacker-cl...
e person beh
75 ★ 33

Frederic Jacobs @FredericJacobs 4h
The whole code-signing/walled-garden thing is supposedly to make you safer but Apple issued a cert for Hacking Team. twitter.com/esizkur/status...
274 ★ 104

Ralf (RPW) @esizkur 4h
Hacking Team had an iOS enterprise developer cert:
Subject: UID=DE9J4B8GTF, CN=iPhone Distribution: HT srl, OU=DE9J4B8GTF, O=HT srl, C=IT
214 ★ 100

https://weakdh.org

BULLRUN

- Code name for NSA project to break crypto by any means possible
- Hack servers to get keys
- Influence policies, standards and specification for commercial public key technologies
- NYT reports NSA has a huge budget for these efforts

Dual_EC_DRBG

- Dual Elliptic Curve Deterministic Random Bit Generator
- PRNG algorithm (ISO 18031 and NIST Standard)
- In 2007, concern about a backdoor
- Required for FIPS 140-2
- BULLRUN revelations implicated Dual_EC_DRBG

> “ NIST strongly recommends that, pending the resolution of the security concerns and the re-issuance of SP 800-90A, the Dual_EC_DRBG, as specified in the January 2012 version of SP 800-90A, no longer be used.”

NIST
http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf

The Problem

- Crypto requires quality data from a PRNG
- Break the PRNG everything else falls
- TLS handshake requires 28 bytes of random data for session master secret
- NSA apparently paid RSA to make Dual_EC_DRBG default PRNG
- This year researchers discovered Dual_EC_DRBG could be backdoored (http://dualec.org)
- Discovered a nonstandard TLS extension in BSAFE implemented by RSA at NSA request to expose more PRNG data

RdRand

- Intel instruction for returning random numbers from on-chip RNG with its own source of entropy
- Compliant with NIST SP 800-90A, FIPS 140-2 and ANSI X9.82
- SP 800-90 requires CTR DRBG, Hash DRBG, HMAC DRBG and Dual_EC_DRBG

> “I am so glad I resisted pressure from Intel engineers to let /dev/random rely only on the RDRAND instruction.”

Theodore Ts'o
https://plus.google.com/+TheodoreTso/posts/SDcoemc9V3J

> “Relying solely on the hardware random number generator which is using an implementation sealed inside a chip which is impossible to audit is a BAD idea.”

Theodore Ts'o
https://plus.google.com/+TheodoreTso/posts/SDcoemc9V3J

OSS Support for RdRand

- Linus rejected petition to remove support from Linux kernel
- FreeBSD has removed support relying instead on Yarrow

FREAK of the Week

- Factoring RSA Export Keys
- SMACK variety
- Legacy of export controls
- Export version of clients
- MITM attack against vulnerable clients and servers
- Proof of concept by INRIA, Microsoft Research and IMDEA

Not a Thing, Right?

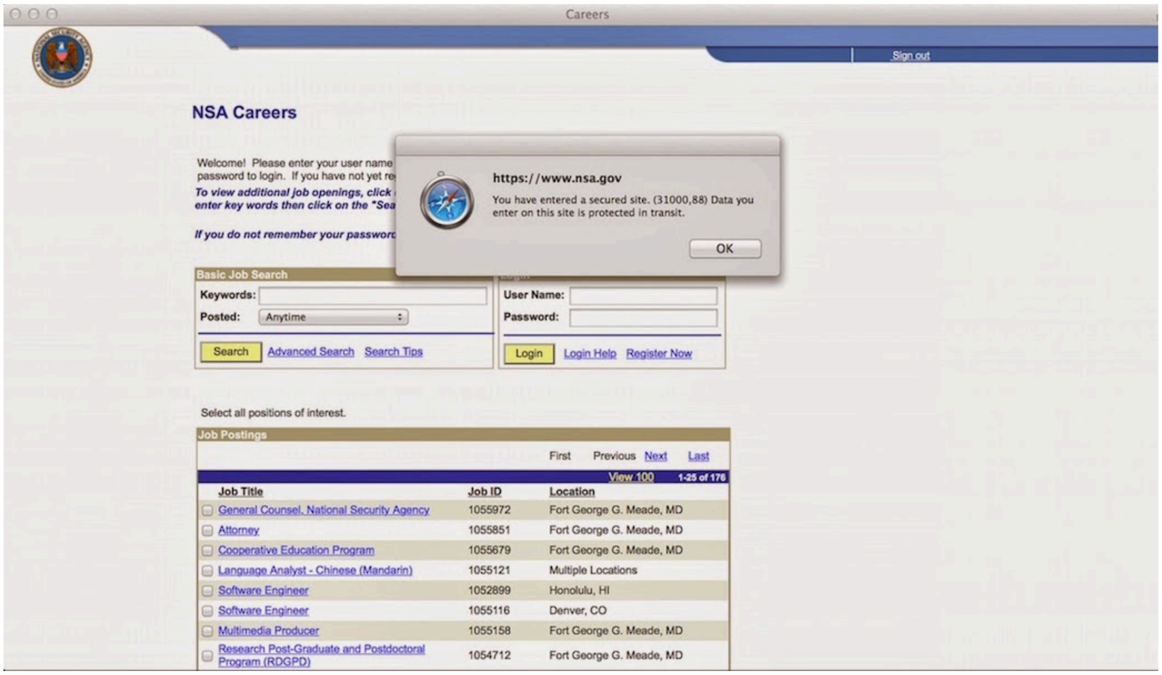
- Modern clients don't negotiate export ciphersuites
- What servers still support export ciphersuites?
- Still requires factoring a 512-bit RSA key or factoring a 40-bit symmetric cipher

Credit: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html?m=1

FREAK Attack

- MITM changes standard RSA ciphersuite request to export request
- OpenSSL/SecureTransport bug
- Attacker factors the RSA modulus to recover decryption key
- Apache mod_ssl reuses export RSA key for the lifetime of the server

Credit: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html?m=1



NSA Careers

Welcome! Please enter your user name
password to login. If you have not yet re

To view additional job openings, click
enter key words then click on the "Sea

If you do not remember your passwor

https://www.nsa.gov

You have entered a secured site. (31000,88) Data you enter on this site is protected in transit.

Basic Job Search

Keywords:

Posted: Anytime

User Name:

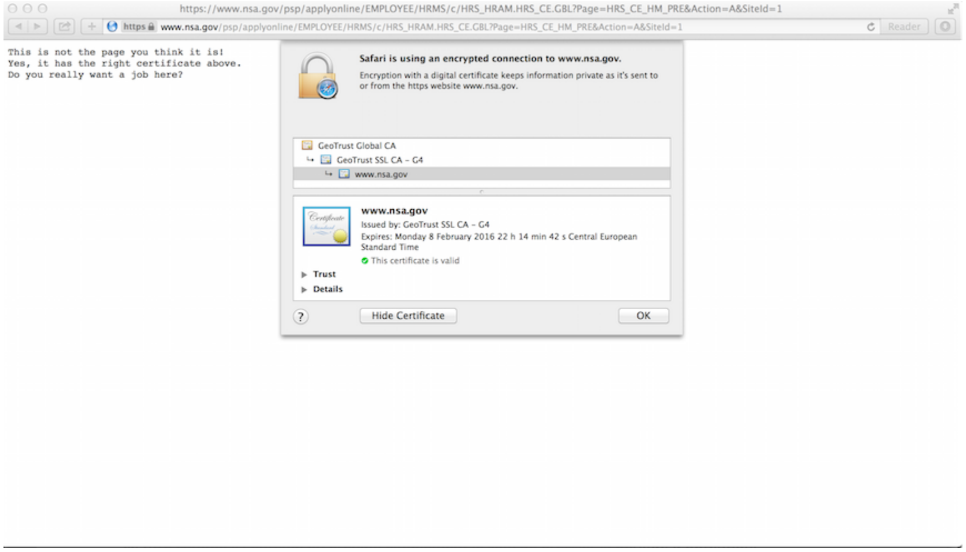
Password:

Select all positions of interest.

Job Postings

1-25 of 176

Job Title	Job ID	Location
□ General Counsel, National Security Agency	1055972	Fort George G. Meade, MD
□ Attorney	1055851	Fort George G. Meade, MD
□ Cooperative Education Program	1055679	Fort George G. Meade, MD
□ Language Analyst - Chinese (Mandarin)	1055121	Multiple Locations
□ Software Engineer	1052899	Honolulu, HI
□ Software Engineer	1055116	Denver, CO
□ Multimedia Producer	1055158	Fort George G. Meade, MD
□ Research Post-Graduate and Postdoctoral Program (RDGPD)	1054712	Fort George G. Meade, MD



https://www.nsa.gov/psp/applyonline/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_CE.GBL?Page=HRS_CE_HM_PRE&Action=A&SiteId=1

www.nsa.gov/psp/applyonline/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_CE.GBL?Page=HRS_CE_HM_PRE&Action=A&SiteId=1

```
This is not the page you think it is!
Yes, it has the right certificate above.
Do you really want a job here?
```

Safari is using an encrypted connection to www.nsa.gov.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.nsa.gov.

GeoTrust Global CA
↳ GeoTrust SSL CA - G4
↳ www.nsa.gov

www.nsa.gov
Issued by: GeoTrust SSL CA - G4
Expires: Monday 8 February 2016 22 h 14 min 42 s Central European Standard Time
✓ This certificate is valid

FREAK Server Vulnerabilities (Random Sample)

- GroupOn
- BusinessInsider
- tinyurl.com
- Kohls.com
- JCPenny.com
- zdnet.com
- cornell.edu
- lg.com
- motorola.com
- sec.gov
- pearson.com

Credit: https://freakattack.com

FREAK Vulnerabilities Client

- OpenSSL (pre-1.0.1k)
- BoringSSL (pre 11/10/14)
- LibReSSL (pre 2.1.2)
- SecureTransport
- SChannel
- Mono (pre 3.12.1)
- IBM JSSE

Credit: https://smacktls.com

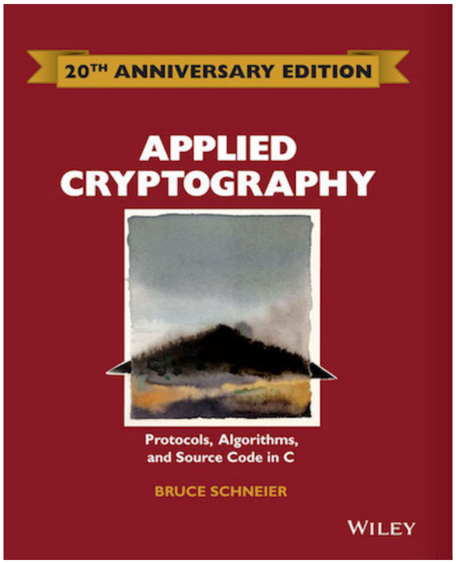
FREAK Vulnerabilities Client

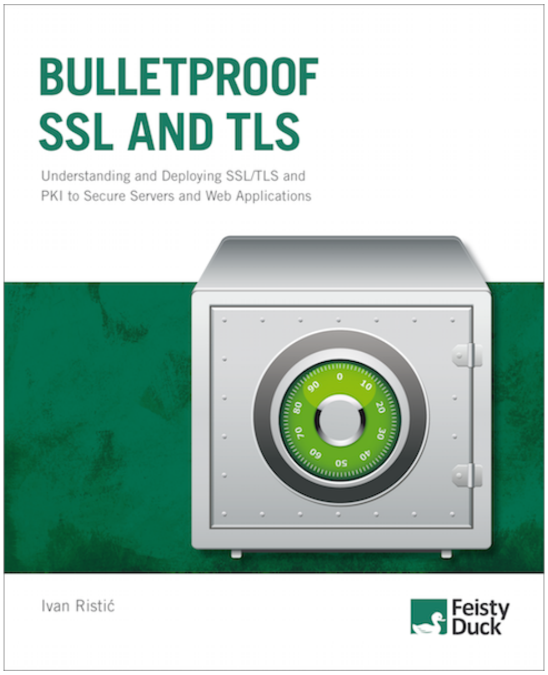
- Safari
- Chrome (OSX and Android)
- Android browser
- Opera
- Blackberry browser
- All versions of Windows
- Test: https://www.smacktls.com/freak/

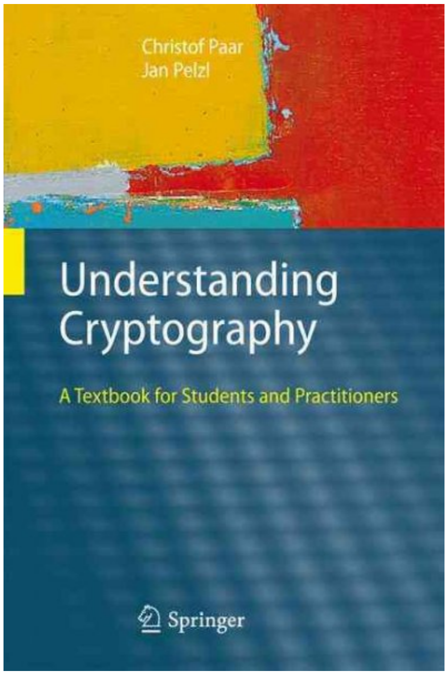
Credit: https://freakattack.com

菩

Books


20TH ANNIVERSARY EDITION
APPLIED CRYPTOGRAPHY
Protocols, Algorithms, and Source Code in C
BRUCE SCHNEIER
WILEY


BULLETPROOF SSL AND TLS
Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications
Ivan Ristić
Feisty Duck

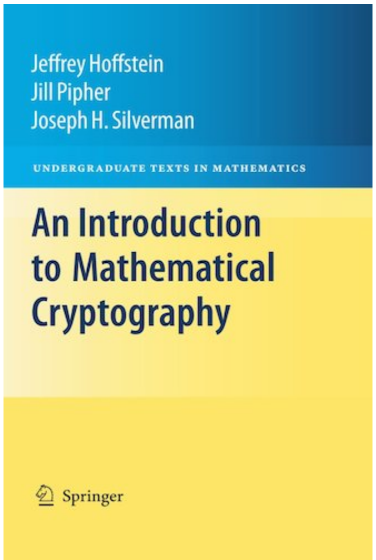


Christof Paar
Jan Pelzl

Understanding Cryptography

A Textbook for Students and Practitioners

Springer



Jeffrey Hoffstein
Jill Pipher
Joseph H. Silverman

UNDERGRADUATE TEXTS IN MATHEMATICS

An Introduction to Mathematical Cryptography

Springer

Questions?

✉ brian@bosatsu.net

@bsletten

g+ http://tinyurl.com/bjs-gplus

bsletten