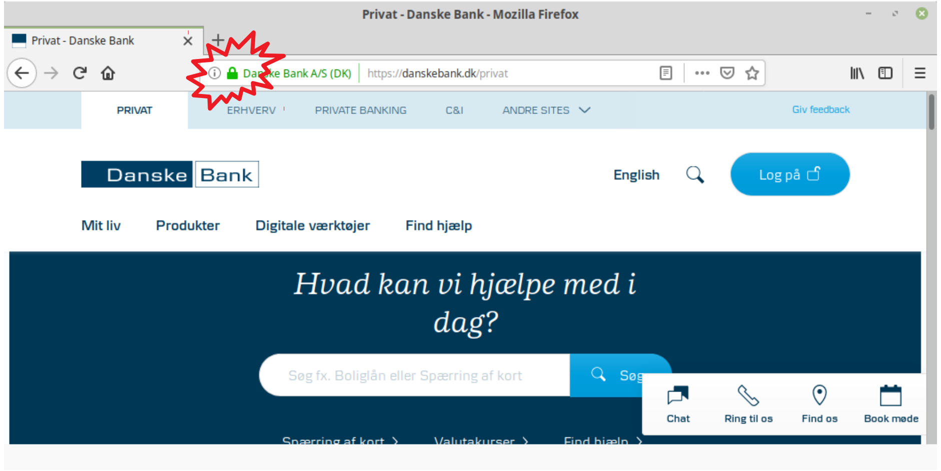
Security in computer networks

CompSys, DIKU 2019/20

Our goal: Secure communication



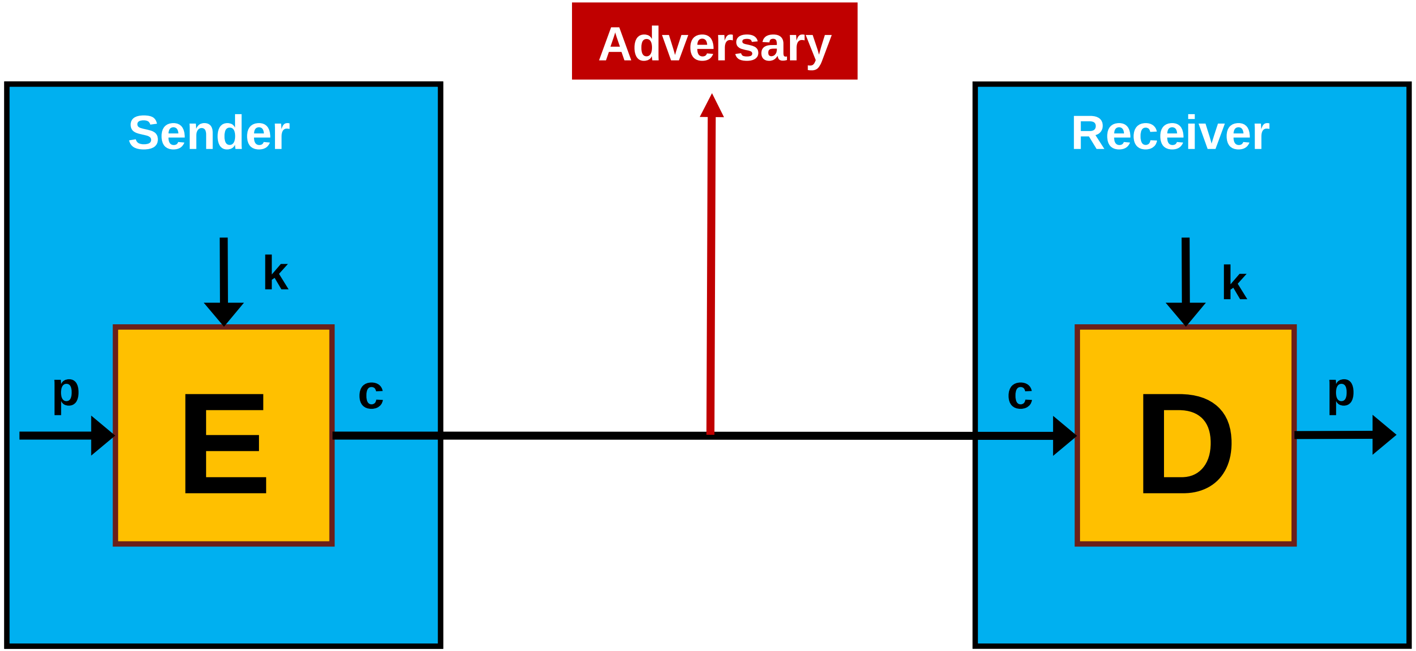
Hvad kan vi hjælpe med i dag?

Agenda

Today: Crypto building blocks

Next time: Crypto protocols

Cryptosystems



Kerckhoffs’ principle

“Il faut qu’il n’exige pas le secret, et qu’il puisse sans inconvénient tomber entre les mains de l’ennemi

The method must not need to be kept secret, and having it fall into the enemy's hands should not cause problems”

Or, the security of a cryptographic algorithm must rest solely in the secrecy of its **key**, not in the secrecy of the algorithm itself

Collaries:

Assume attacker knows the algorithm
Make it available for public analysis
Protect the key!

Auguste
Kerckhoffs
(1835 – 1903)

Security goals

Confidentiality	– prevent eavesdropping
Integrity	– prevent modifications
Authentication	– prevent impersonation

Goal #1: Confidentiality

Symmetric cryptosystems

Symmetric cryptosystems

Stream ciphers

One time pad

If *k* random, |*k*| >= |*p*|, never reused, and kept secret, then then impossible to decrypt or break without knowing the key (Shannon, 1949)

Key:	0	1	0	1	1	1	0	0	1	0	
Plaintext:	1	1	0	0	0	1	1	0	0	0	⊕
Ciphertext:	1	0	0	1	1	0	1	0	1	0	

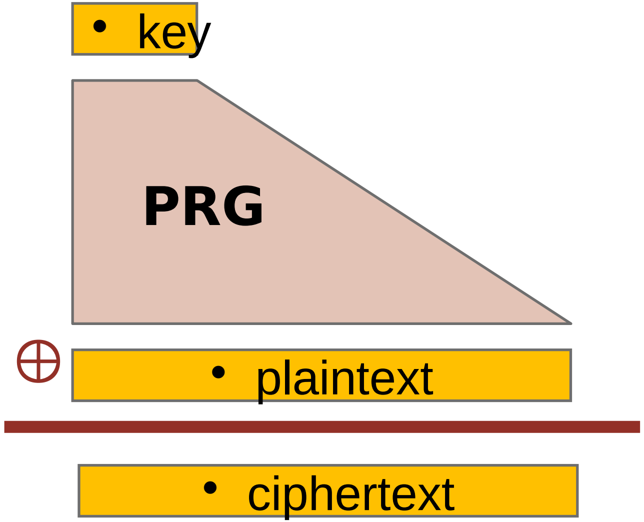
Towards modern stream ciphers

Problem

OTP key as long as plaintext

Solution

Generate pseudo random keystream



1st rule of stream ciphers

Never reuse key

$$C_1 \leftarrow P_1 \oplus PRG(k)$$

$$C_2 \leftarrow P_2 \oplus PRG(k)$$

$$C_1 \oplus C_2 \rightarrow P_1 \oplus P_2$$

$$P_1 \oplus P_2 \rightarrow P_1 , P_2$$

Solution: Initialisation Vector (IV)

For each message

- Generate IV
- Mix k with IV
- Generate keystream PRG(k+IV) and encrypt
- Send c and IV (in plaintext)

Change k before IVs run out

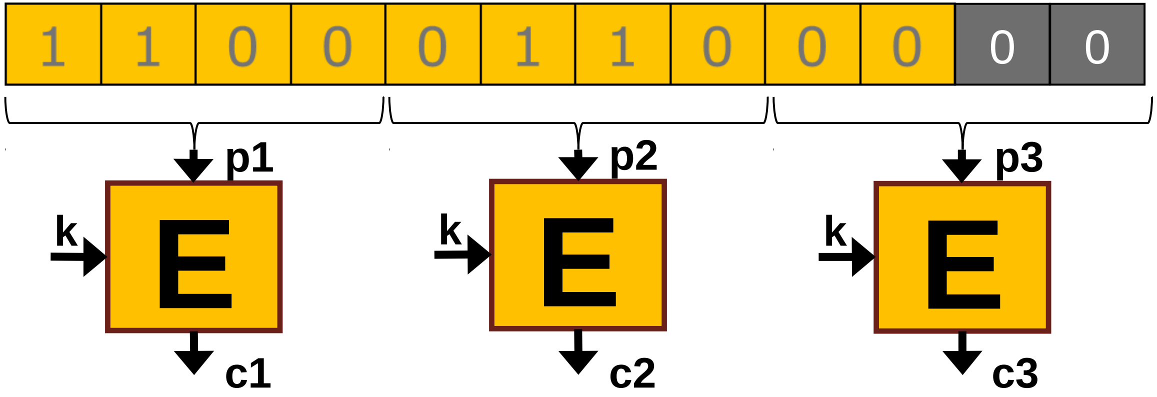
Stream ciphers in the wild

Block ciphers

Block ciphers

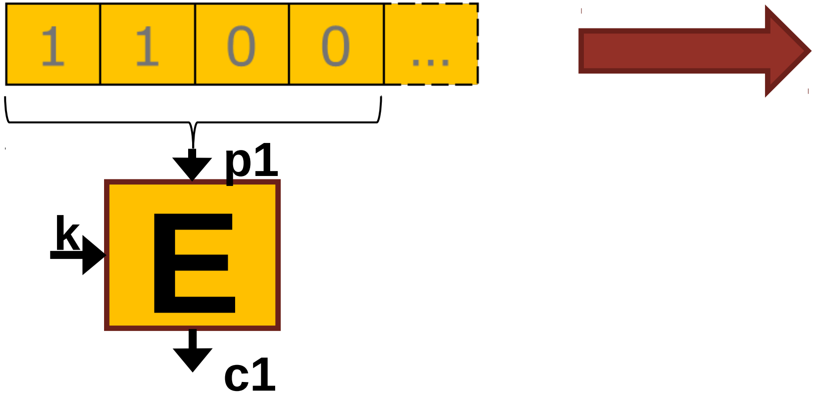
One block at a time – as oppossed to one bit at a time

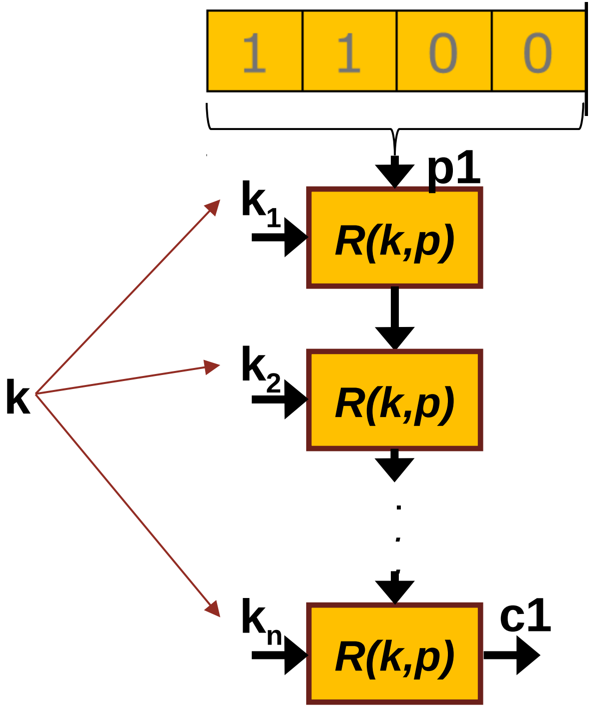
- **padding**



One block at a time

Blocks, rounds founction, key schedule, iterations



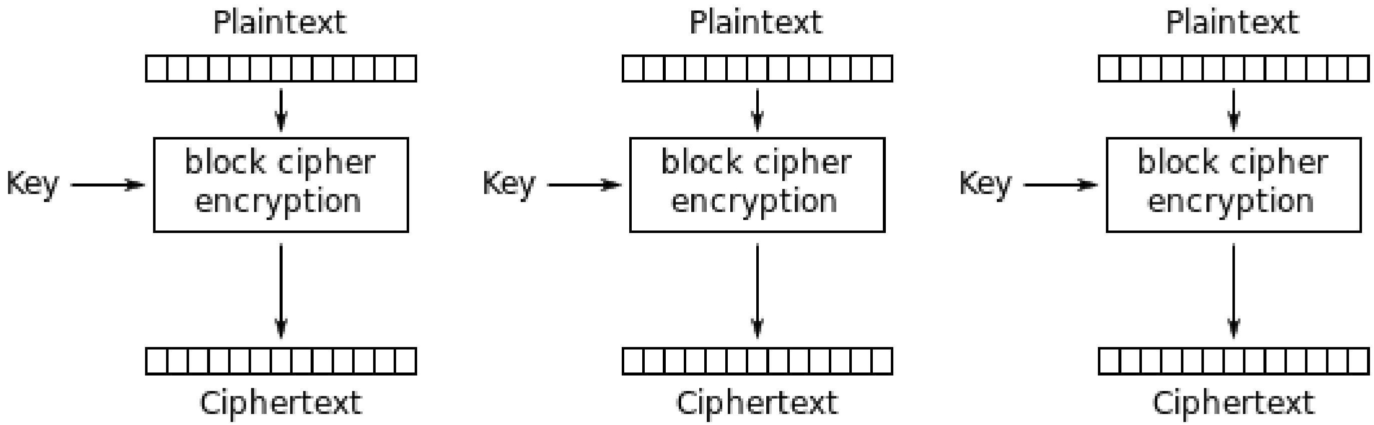


DES, AES

- DES
  - Key 64, block 64, rounds 16
- AES
  - Keys 128/192/256, block 128, rounds 10/12/14

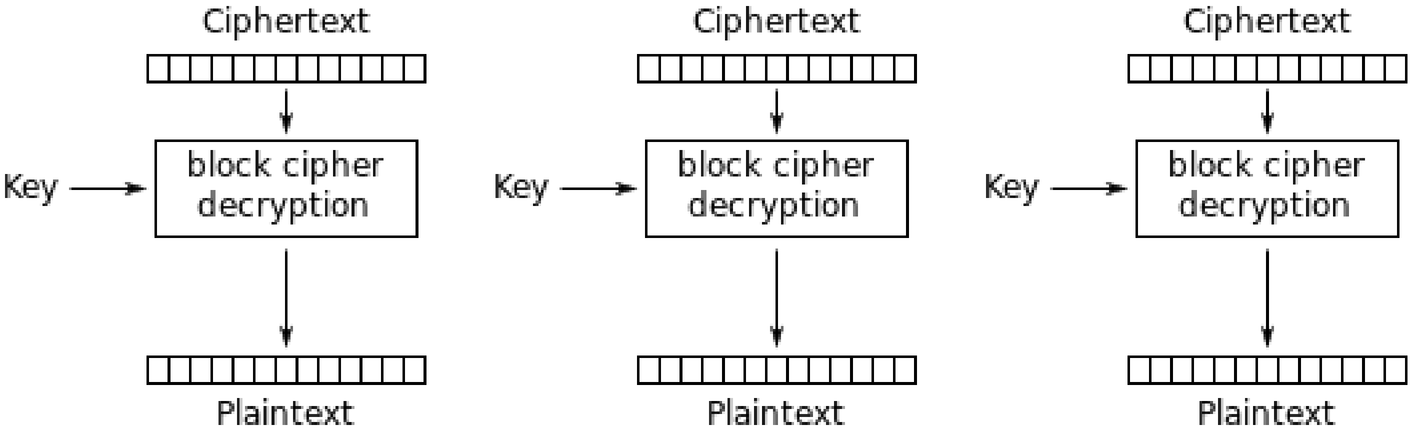
Modes of operation

Electronic Codebook (ECB)



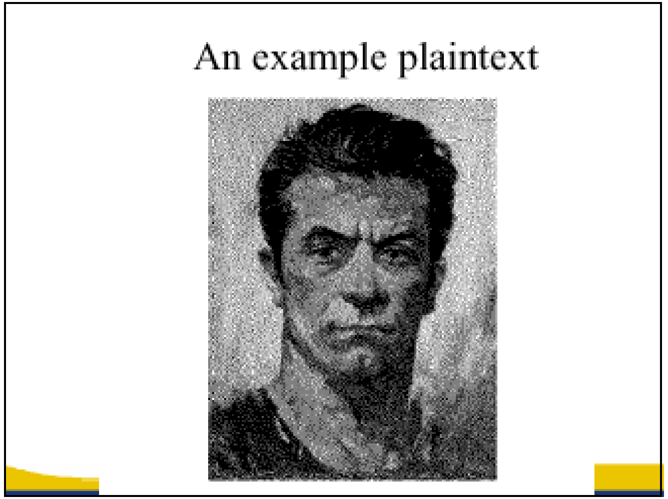
Electronic Codebook (ECB) mode encryption

ECB decyption

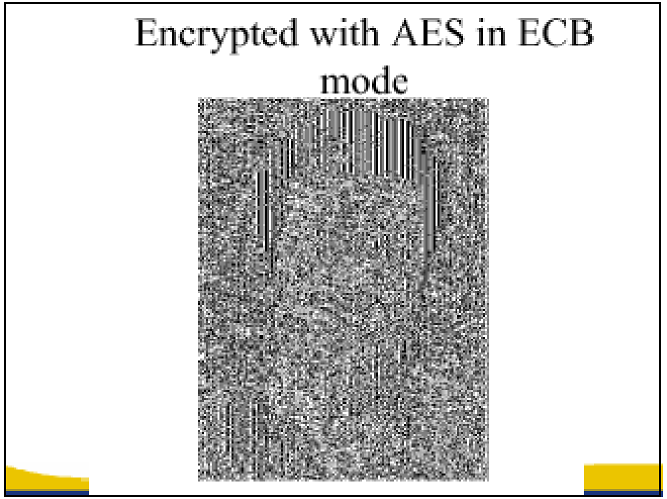


Electronic Codebook (ECB) mode decryption

If p1 = p2, then c1 = c2

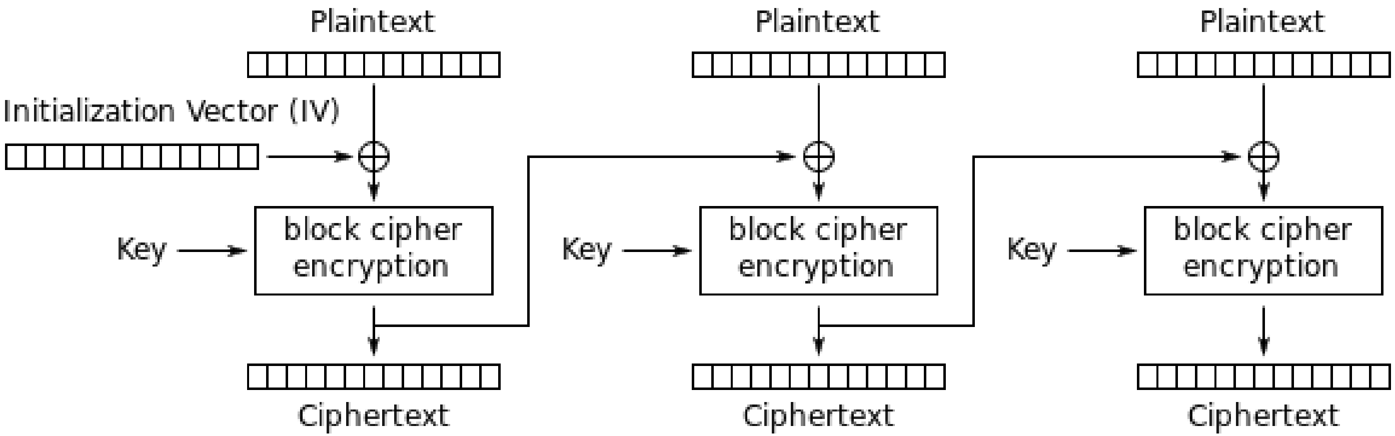


An example plaintext



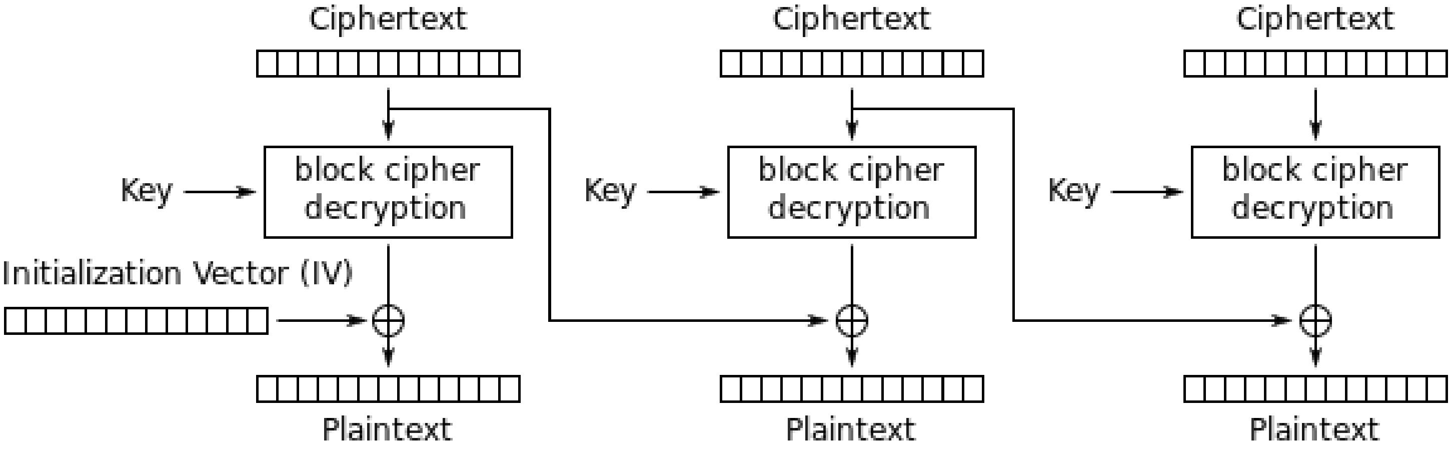
Encrypted with AES in ECB mode

Cipher Block Chaining



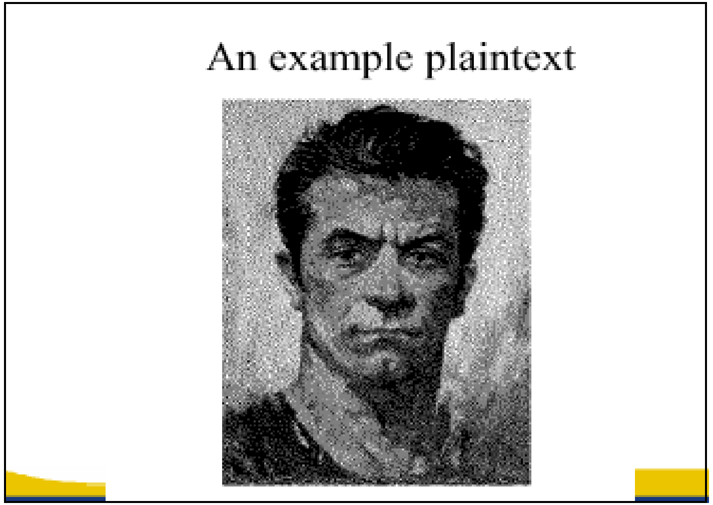
Cipher Block Chaining (CBC) mode encryption

CBC decryption

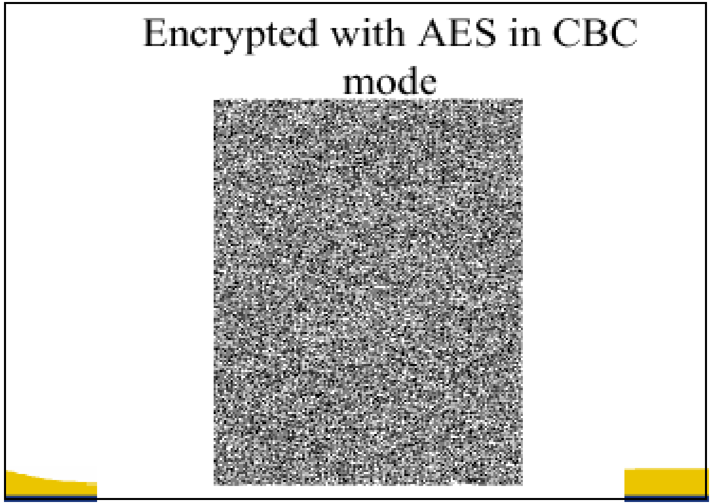


Cipher Block Chaining (CBC) mode decryption

Better

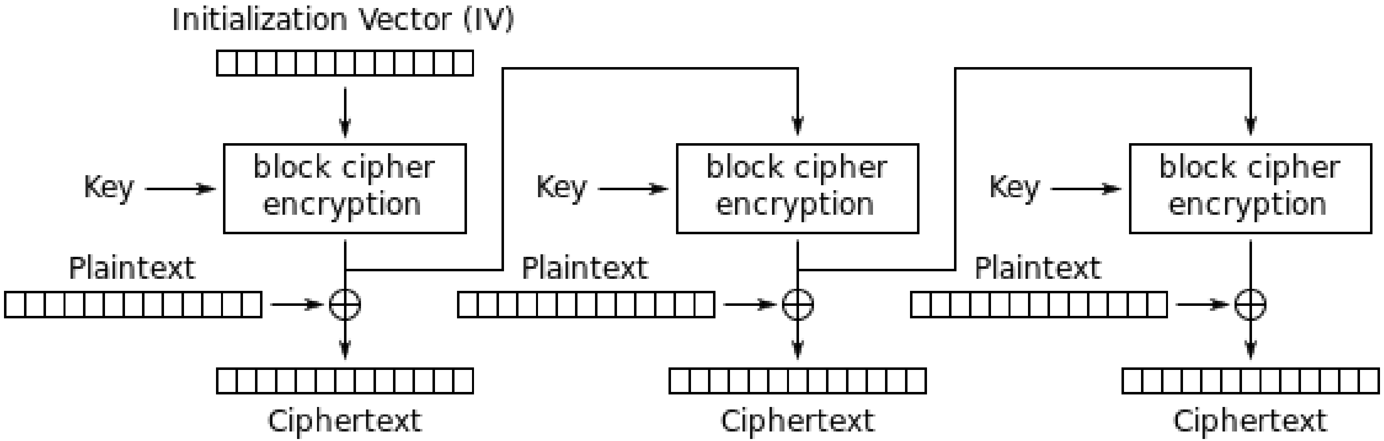


An example plaintext



Encrypted with AES in CBC mode

Output Feedback



Output Feedback (OFB) mode encryption

Security goals revisited

“Susceptibility to malicious insertions and modifications. Because each symbol is separately enciphered, an active interceptor who has broken the code can splice together pieces of previous messages and transmit a spurious new message that may look authentic.” - Phleeger & Phleeger in Security in Computing, Pearson, 2003

Is this a disadvantage of stream cipher? Why, why not?

Security goal of encryption: Confidentiality

Status

Confidentiality: Check!

Integrity: Missing

Message authentication code (MAC)

Message authentication code

Goal: Provide integrity

Process

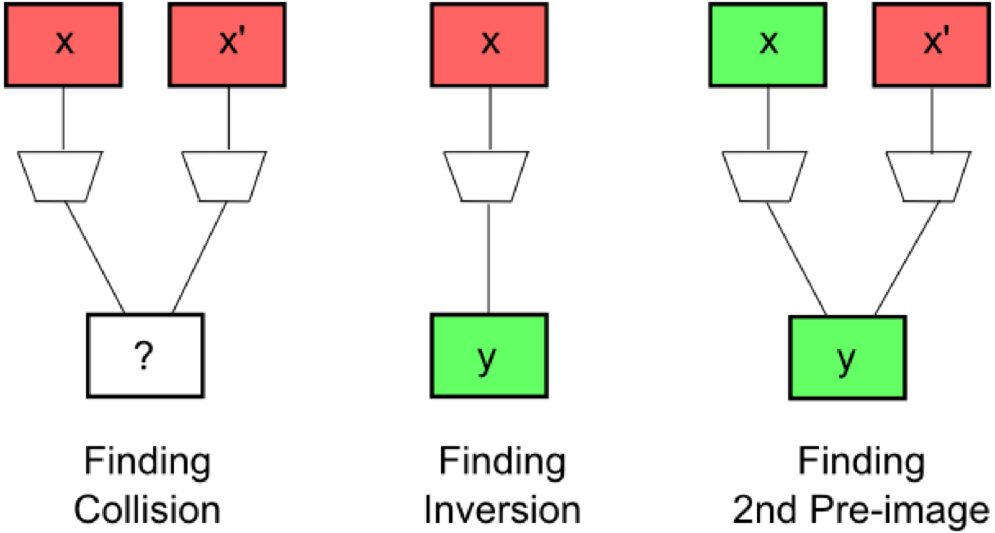
Choose a cryptographic hash funciton h : $\{0,1\}^x \rightarrow \{0,1\}^n$

Sender: Send h(m),m

Receiver: Calculate h(m) and verify it matches h(m)

Examples MD5 (n = 128), SHA-256 (n = 256)

Cryptographic hash functions



Hash-based MAC (HMAC)

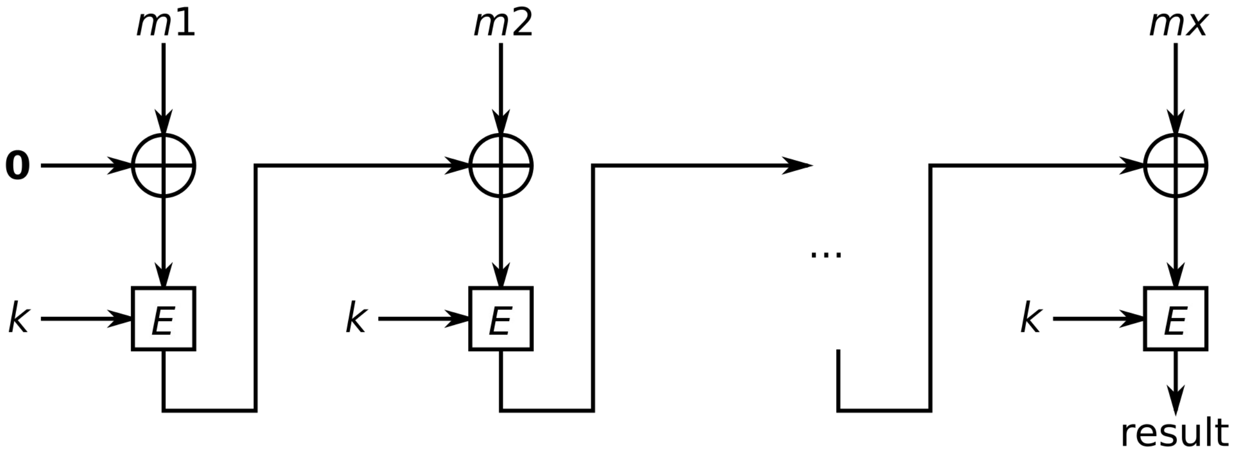
RFC2104: Hash-based MAC

HMAC(h,k,m) =

$$h\ (\ (k \oplus opad) \parallel h\ ((k \oplus ipad) \parallel m)$$

HMAC provides integrity and authenticity

CBC-MAC



Car keys

Your car key sends the code for ”open the door”, together with a MAC, to the car whenever you press the button.

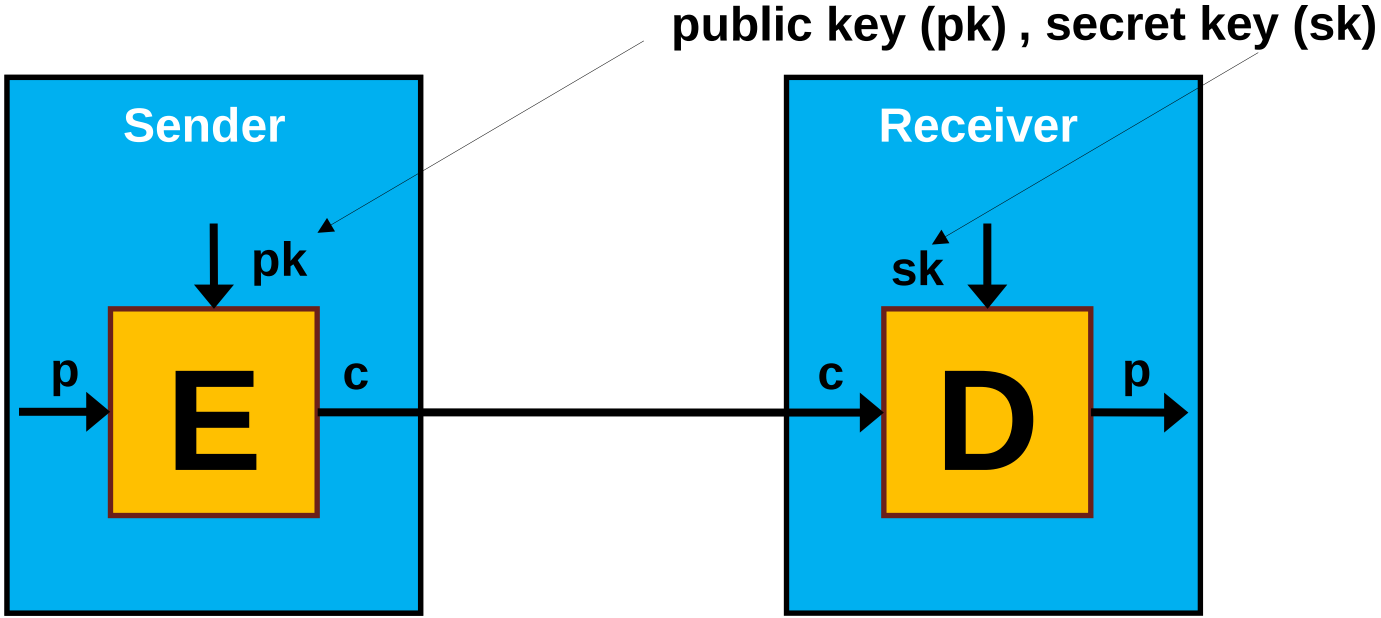
What could go wrong?

Replay attack: attacker records message and replays it later

We need some freshness: a timestamp or nonce

Public-key cryptography

Or, asymmetric encryption



Analogy: Combination locks

Bob sends out locks with combination he only knows

Alice picks one of Bob's locks, places her message in a box and locks it with Bob's lock

Bob is the only one who can open the box now

No pre-shared key!

- Bob
  - Publish public key, protect private key
- Alice
  - Encrypt message with Bob’s public key
- Bob
  - Decrypts with his private key

Rivest Shamir Adleman (RSA), 1978

Key generation

Encryption

Decryption

RSA key generation

Choose two large prime numbers p, q

Compute n = pq, z = (p-1)(q-1)

Choose e (with e<n) that has no common factors with z

Choose d such that ed mod z = 1

Public key is (n,e). Private key is (n,d).

RSA encryption and decryption

Public key (n,e), private key (d)

Encryption

- Transform M to m in {0,n-1}
- Compute $c = m^e \pmod n$

Deccryption

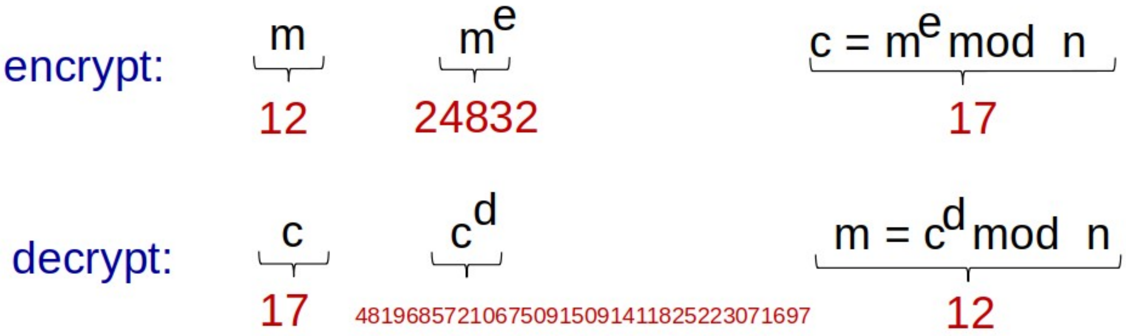
- Compute $m = c^d \pmod n$
- Reverse transformation to get M

RSA example

Alice chooses p=5, q=7. Then n=35, z=24.

Sets e=5 (so e, z relatively prime).

And d=29 (so ed-1 exactly divisible by z).



encrypt: $\underbrace{m}_{12}$ $\underbrace{m^e}_{24832}$ $\underbrace{c = m^e \bmod n}_{17}$

decrypt: $\underbrace{c}_{17}$ $\underbrace{c^d}_{481968572106750915091411825223071697}$ $\underbrace{m = c^d \bmod n}_{12}$

RSA security

The RSA problem: Find the eth root of m^e mod n

Most promising method, integer factorisation:

- Given N = pq, p, q prime, factor n
- Then, from public e, re-generate d

Integer factorisation is a “hard” problem

- No polynomial-time algorithm found, non-existance not proved either
- Largest number factored: 768 bits long (RSA-768, 2010) $\Rightarrow$ Choose n > 2048 bits

RSA in practice

Hybrid cryptography

- Use public-key encryption to encrypt and exchange symmetric keys
- Use symmetric encryption for bulk encryption

Reverse = digital signature

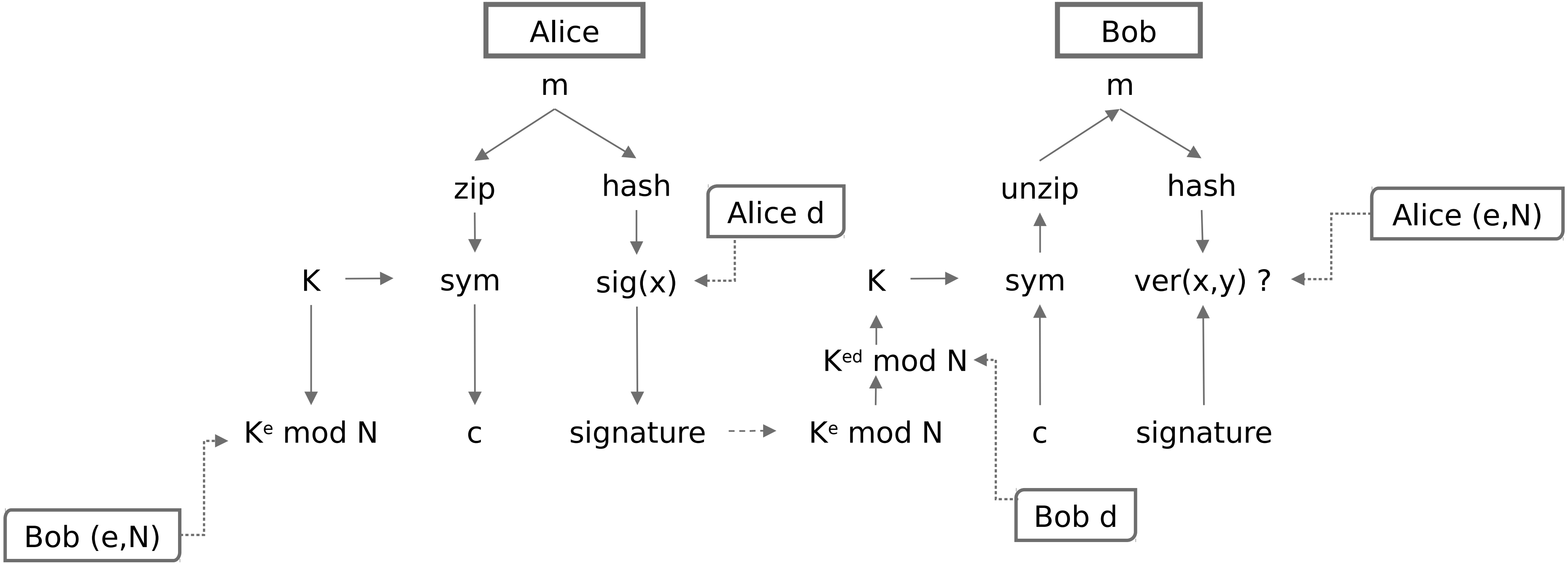
Public key (n,e), private key (d)

Signature: sig(m) = m^d (mod n)

Verify: ver(m,sig(m)) = true iff m = $(m^d)^e$ (mod n)

Remember h(m)

Putting it all togehter



Next time, real-world crypto protocols

Key management

Many keys to protect

Master key

Session key

Signature key

Data encryption key

Key encryption key

...

Protect during entire lifecycle

Generation

Exchange

Storage/backup

Use

Expiration

Revocation

Destruction

Key exchange options include

- Pre-distribution
    - Generated and distributed “ahead of time” e.g. physically
- Distribution
    - Generated by a trusted third party (TTP) and sent to all parties
- Agreement
    - Generated by all parties working together
- Asymmetric
    - Is *e* really yours?

Is e really yours?

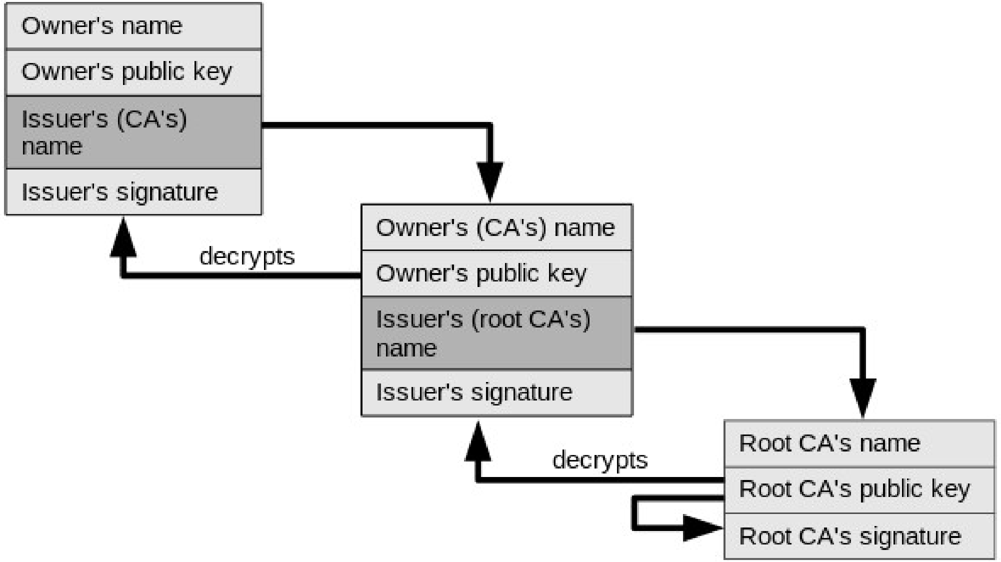
Public-key infrastructure (PKI)

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

X.509 format for certificates include:

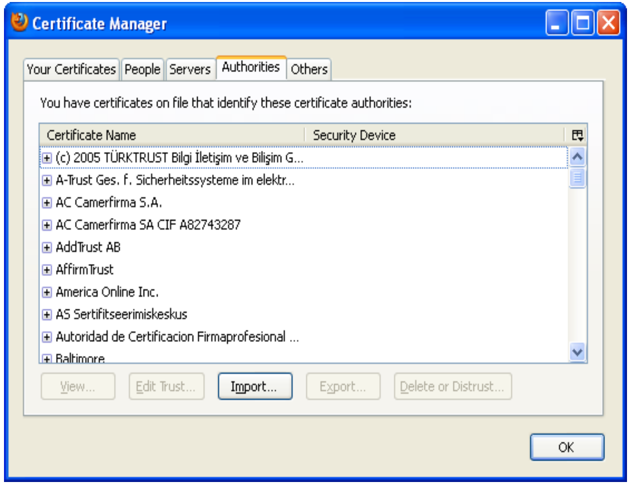
Serial number	– unique identification of certificate
Valid-From/To	– lifespan of the certificate
Subject	– the entity/person/machine/etc. identified
Public key	– the entity's public key
Signature	– the actual signature of the issuer

Chain of trust



Trust in browsers

Browsers come pre-configured with a set of root CAs. Do you trust all these CAs (to authenticate properly, to avoid/inform of breaches)?



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim G...	
A-Trust Ges. f. Sicherheitssysteme im elektr...	
AC Camerfirma S.A.	
AC Camerfirma SA CIF A82743287	
AddTrust AB	
AffirmTrust	
America Online Inc.	
AS Sertifitseerimiskeskus	
Autoridad de Certificacion Firmaprofesional ...	
Baltimore	

Wrap-up

Security goals achieved

Confidentiality

Integrity

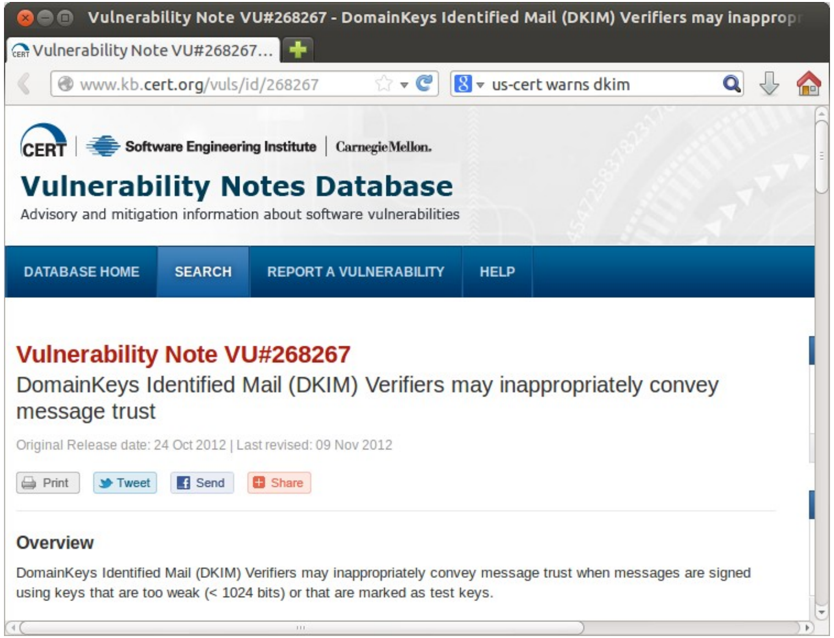
Authentication

Non-repudiation

CHECK!

But crypto can still fail

Small keys fail



Vulnerability Note VU#268267 - DomainKeys Identified Mail (DKIM) Verifiers may inapprop
Vulnerability Note VU#268267...
www.kb.cert.org/vuls/id/268267
us-cert warns dkim
CERT
Software Engineering Institute
CarnegieMellon.
DATABASE HOME
SEARCH
REPORT A VULNERABILITY
HELP
Print
Tweet
Send
Share

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

Vulnerability Note VU#268267

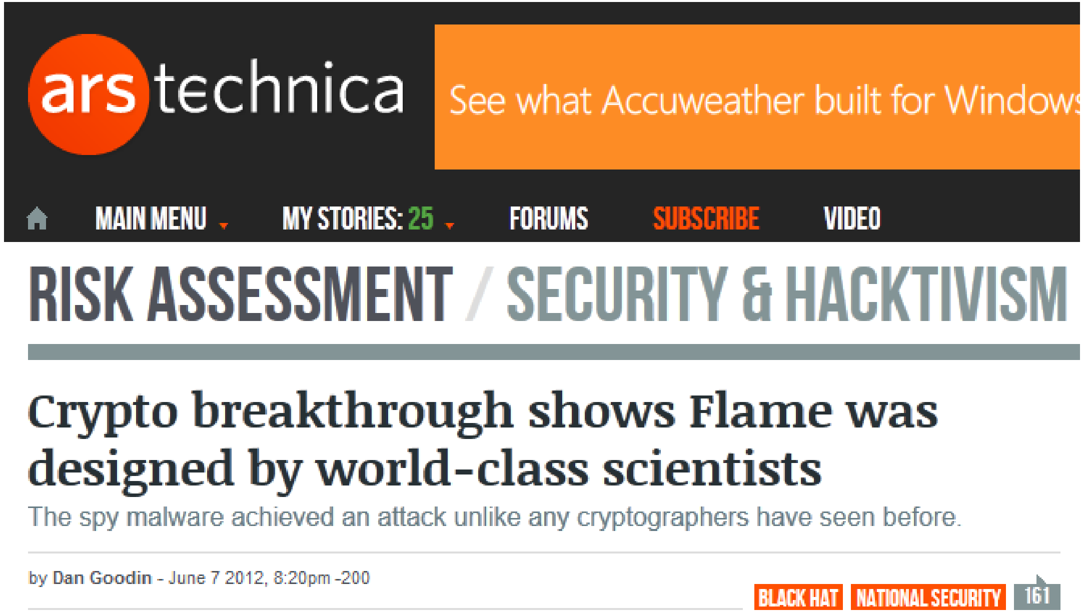
DomainKeys Identified Mail (DKIM) Verifiers may inappropriately convey message trust

Original Release date: 24 Oct 2012 | Last revised: 09 Nov 2012

Overview

DomainKeys Identified Mail (DKIM) Verifiers may inappropriately convey message trust when messages are signed using keys that are too weak (< 1024 bits) or that are marked as test keys.

Collision fail

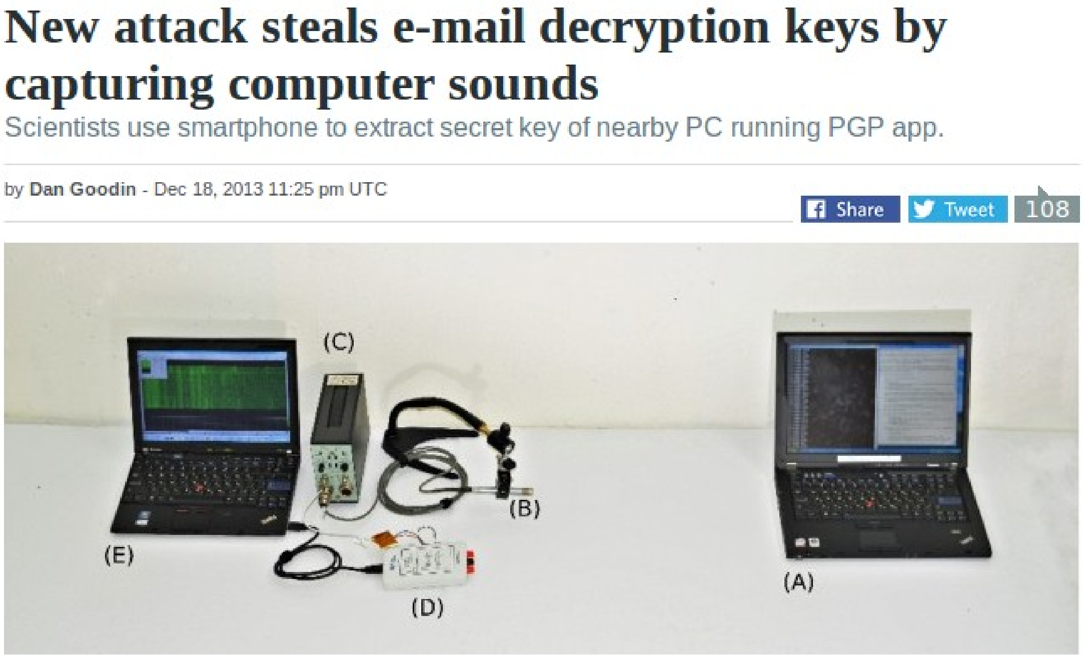


Crypto breakthrough shows Flame was designed by world-class scientists

The spy malware achieved an attack unlike any cryptographers have seen before.

by Dan Goodin - June 7 2012, 8:20pm -200

Impressive fail

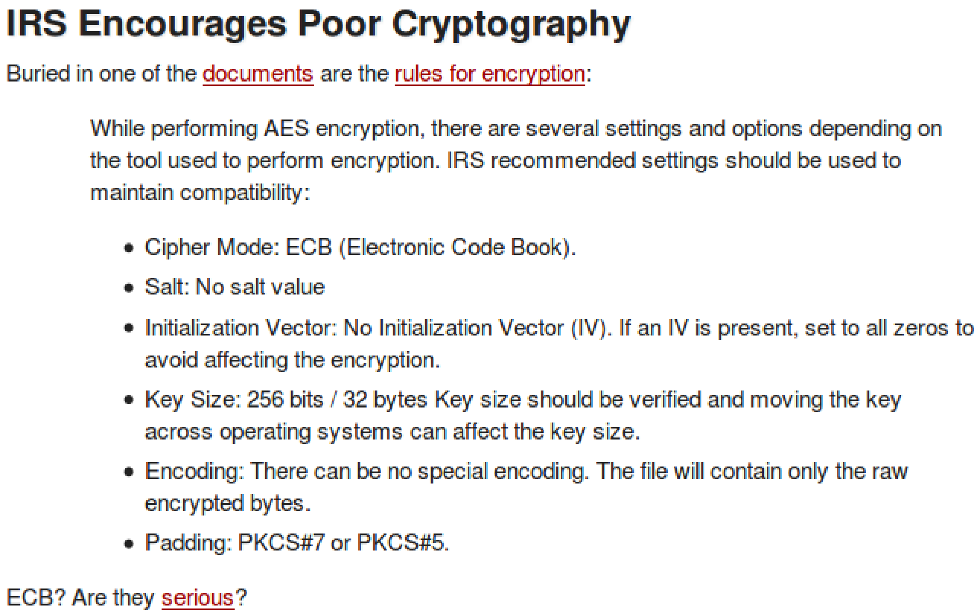


New attack steals e-mail decryption keys by capturing computer sounds

Scientists use smartphone to extract secret key of nearby PC running PGP app.

by **Dan Goodin** - Dec 18, 2013 11:25 pm UTC

Bad choice fail



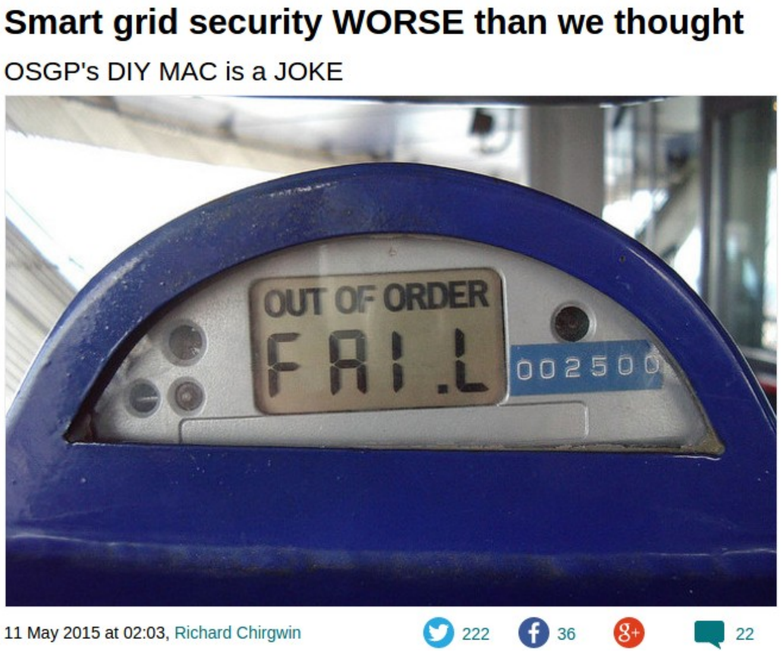
IRS Encourages Poor Cryptography

Buried in one of the documents are the rules for encryption:

> While performing AES encryption, there are several settings and options depending on the tool used to perform encryption. IRS recommended settings should be used to maintain compatibility:
>
> - Cipher Mode: ECB (Electronic Code Book).
> - Salt: No salt value
> - Initialization Vector: No Initialization Vector (IV). If an IV is present, set to all zeros to avoid affecting the encryption.
> - Key Size: 256 bits / 32 bytes Key size should be verified and moving the key across operating systems can affect the key size.
> - Encoding: There can be no special encoding. The file will contain only the raw encrypted bytes.
> - Padding: PKCS#7 or PKCS#5.

ECB? Are they serious?

DIY fail

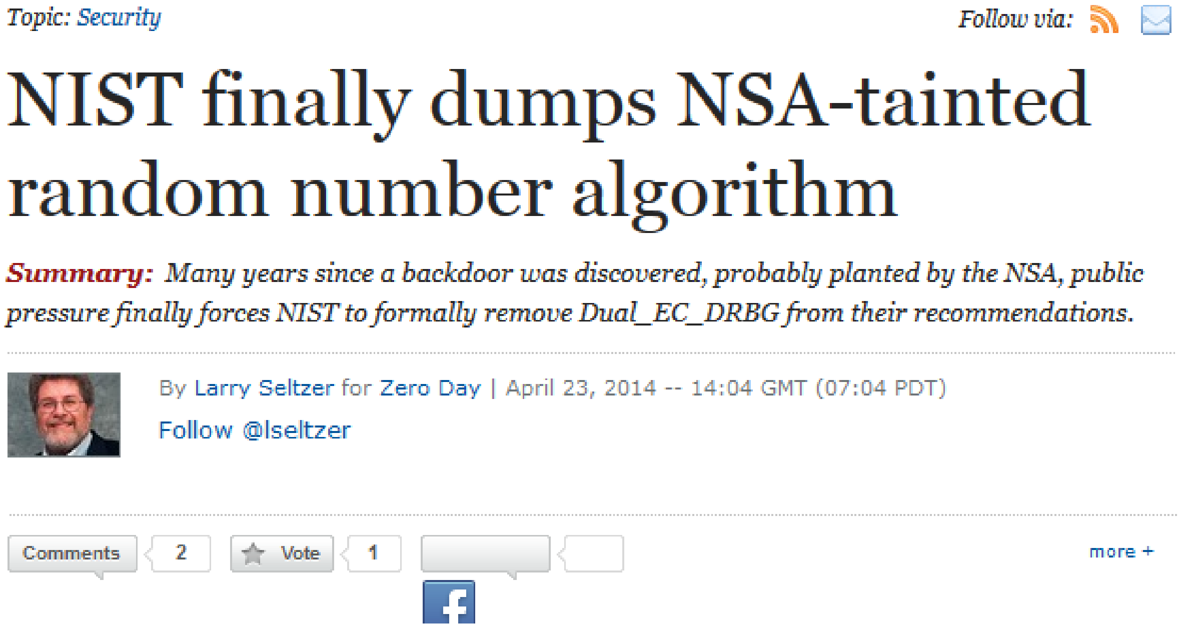


Smart grid security WORSE than we thought

OSGP's DIY MAC is a JOKE

11 May 2015 at 02:03, Richard Chirgwin

Backdoor fail



Topic: Security

Follow via:

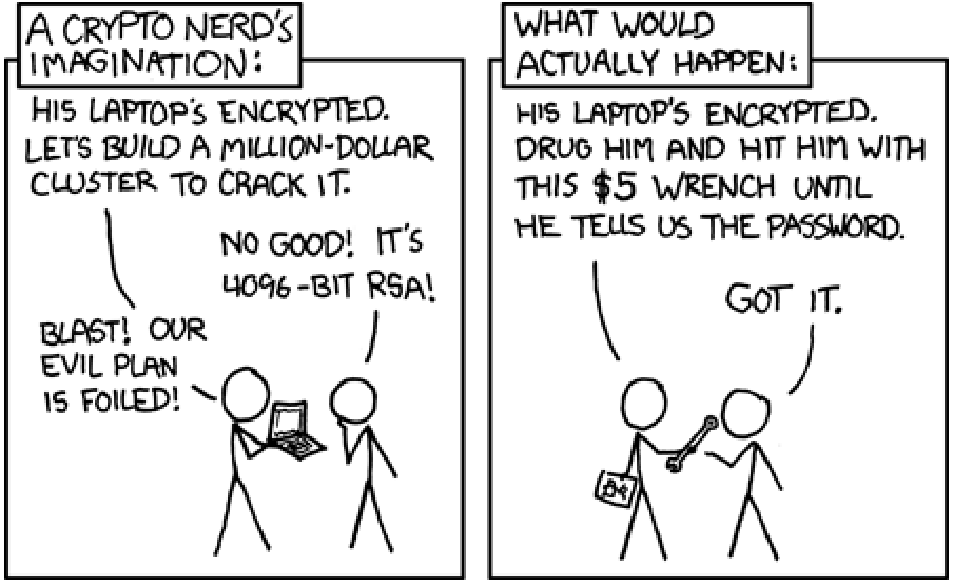
NIST finally dumps NSA-tainted random number algorithm

Summary: *Many years since a backdoor was discovered, probably planted by the NSA, public pressure finally forces NIST to formally remove Dual_EC_DRBG from their recommendations.*

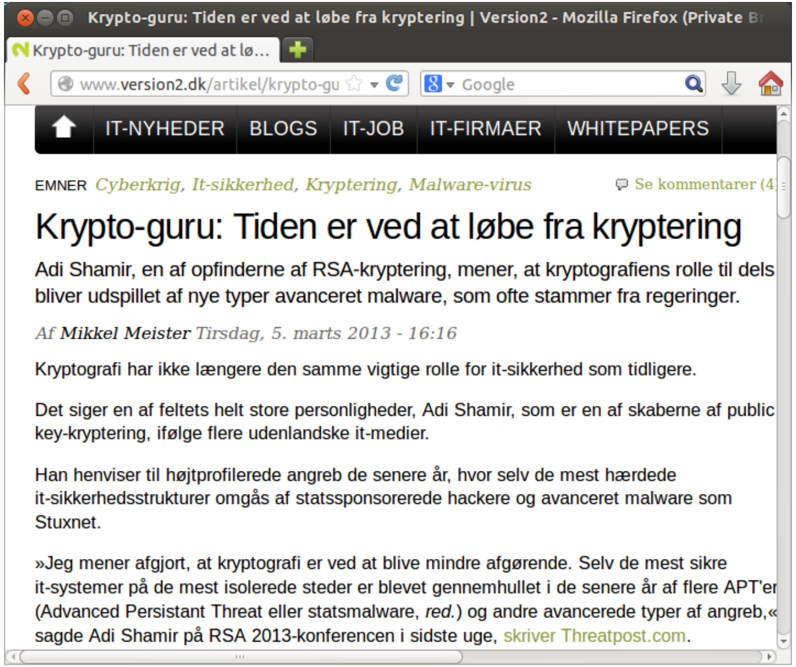
By Larry Seltzer for Zero Day | April 23, 2014 -- 14:04 GMT (07:04 PDT)

Follow @lseltzer

Real-world fail


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

(Malware fail)


Krypto-guru: Tiden er ved at løbe fra kryptering | Version2 - Mozilla Firefox (Private B
Krypto-guru: Tiden er ved at lø…
www.version2.dk/artikel/krypto-gu
Google
IT-NYHEDER
BLOGS
IT-JOB
IT-FIRMAER
WHITEPAPERS

EMNER *Cyberkrig, It-sikkerhed, Kryptering, Malware-virus* Se kommentarer (4

Krypto-guru: Tiden er ved at løbe fra kryptering

Adi Shamir, en af opfinderne af RSA-kryptering, mener, at kryptografiens rolle til dels bliver udspillet af nye typer avanceret malware, som ofte stammer fra regeringer.

Af ***Mikkel Meister*** *Tirsdag, 5. marts 2013 - 16:16*

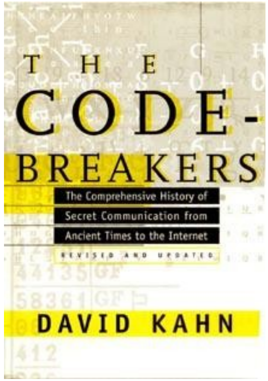
Kryptografi har ikke længere den samme vigtige rolle for it-sikkerhed som tidligere.

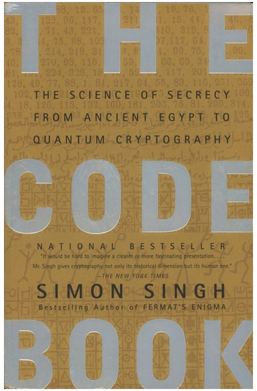
Det siger en af feltets helt store personligheder, Adi Shamir, som er en af skaberne af public key-kryptering, ifølge flere udenlandske it-medier.

Han henviser til højtprofilerede angreb de senere år, hvor selv de mest hærdede it-sikkerhedsstrukturer omgås af statssponsorerede hackere og avanceret malware som Stuxnet.

»Jeg mener afgjort, at kryptografi er ved at blive mindre afgørende. Selv de mest sikre it-systemer på de mest isolerede steder er blevet gennemhullet i de senere år af flere APT'er (Advanced Persistant Threat eller statsmalware, *red.*) og andre avancerede typer af angreb,« sagde Adi Shamir på RSA 2013-konferencen i sidste uge, skriver Threatpost.com.

Suggested reading


THE
CODE-
BREAKERS
The Comprehensive History of
Secret Communication from
Ancient Times to the Internet
REVISED AND UPDATED
DAVID KAHN


THE
THE SCIENCE OF SECRECY
FROM ANCIENT EGYPT TO
QUANTUM CRYPTOGRAPHY
CODE
NATIONAL BESTSELLER
"It would be hard to imagine a clearer or more fascinating presentation. . . .
Mr. Singh gives cryptography not only its historical dimension but its human one."
—THE NEW YORK TIMES
SIMON SINGH
Bestselling Author of FERMAT'S ENIGMA
BOOK