INF3510 Information Security
University of Oslo
Spring 2018

Lecture 3

Cryptography

University of Oslo, spring 2018

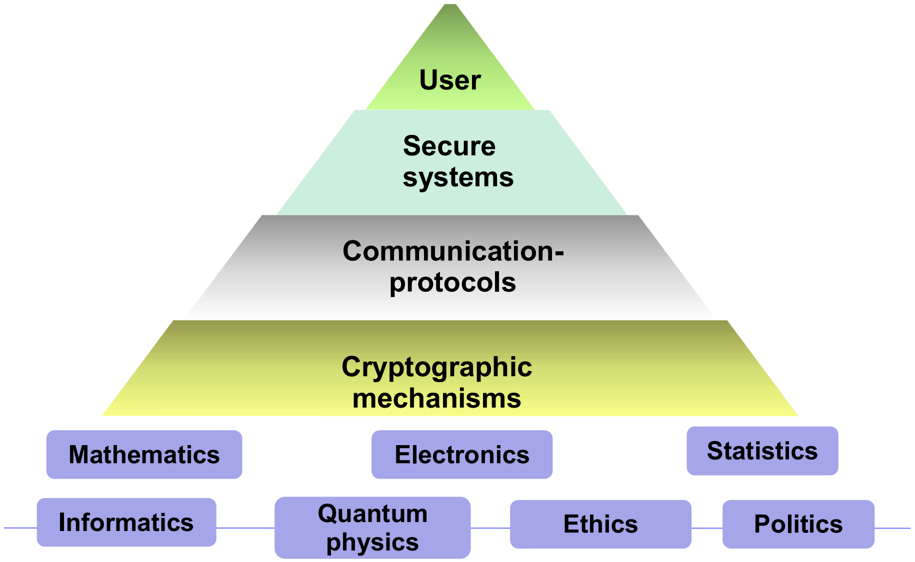
Leif Nilsen

Outline

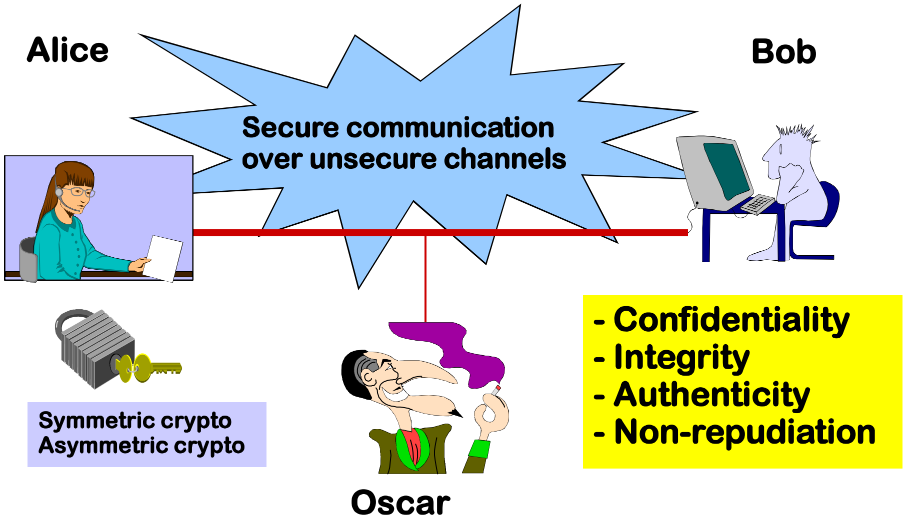
- What is cryptography?
- Brief crypto history
- Security issues
- Symmetric cryptography
  - Stream ciphers
  - Block ciphers
  - Hash functions
- Asymmetric cryptography
  - Factoring based mechanisms
  - Discrete Logarithms
  - Digital signatures
  - Quantum Resistant Crypto

Want to learn more?
Look up UNIK 4220

The security pyramid

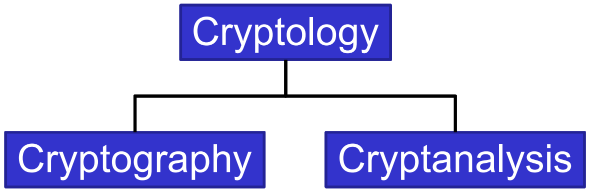


What is cryptology?



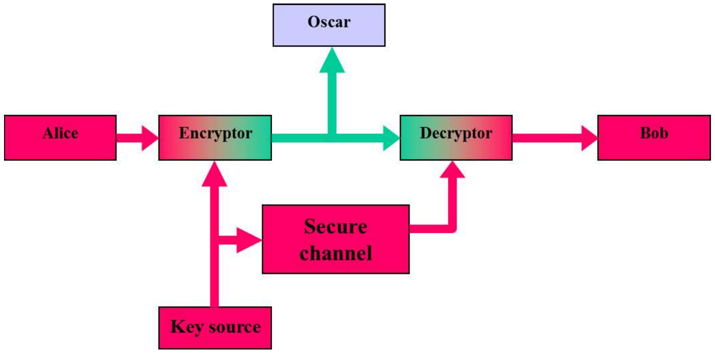
- Confidentiality
- Integrity
- Authenticity
- Non-repudiation

Terminology

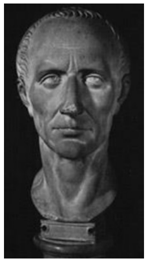


- **Cryptography** is the science of secret writing with the goal of hiding the meaning of a message.
- **Cryptanalysis** is the science and sometimes art of *breaking* cryptosystems.

Model of symmetric cryptosystem



Caesar cipher



Example: Caesar cipher

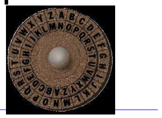
P = {`abcdefghijklmnopqrstuvwxyz`}

C = {`DEFGHIJKLMNOPQRSTUVWXYZABC`}

Plaintext: `kryptologi er et spennende fag`

Chiphertext: `NUBSWRORJL HU HT VSHQQHQGH IDJ`

Note: Caesar chipher in this form does not include a variable key, but is an instance of a "shift-cipher" using key $K = 3$.



Numerical encoding of the alphabet

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

p	q	r	s	t	u	v	w	x	y	z	æ	ø	å
14	16	17	18	19	20	21	22	23	24	25	26	27	28

Using this encoding many classical crypto systems can be expressed as algebraic functions over Z_{26} (English alphabet) or Z_{29} (Norwegian alphabet)

Shift cipher

Let **P = C =** Z_{26}. For $0 \le K \le 25$, we define

$$E(x, K) = x + K \pmod{26}$$

and

$$D(y, K) = y - K \pmod{26}$$

$(x, y \in Z_{26})$

Question: What is the size of the key space?

Puzzle: ct =

LAHYCXPAJYQHRBWNNMNMOXABNLDANLXVVDWRLJCRXWB

Find the plaintext!

Exhaustive search

```
For[i=0, i<26, i++, Print["Key = ", i, " Plain = ", decrypt[ct,1,i]]]
Key = 0 Plain = LAHYCXPAJYQHRBWNNMNMOXABNLDANLXVVDWRLJCRXWB
Key = 1 Plain = KZGXBWOZIXPGQAVMMLMLNWZAMKCZMKWUUCVQKIBQWVA
Key = 2 Plain = JYFWAVNYHWOFPZULLKLKMVYZLJBYLJVTTBUPJHAPVUZ
Key = 3 Plain = IXEVZUMXGVNEOYTKKJKJLUXYKIAXKIUSSATOIGZOUTY
Key = 4 Plain = HWDUYTLWFUMDNXSJJIJIKTWXJHZWJHTRRZSNHFYNTSX
Key = 5 Plain = GVCTXSKVETLCMWRIIHIHJSVWIGYVIGSQQYRMGEXMSRW
Key = 6 Plain = FUBSWRJUDSKBLVQHHGHGIRUVHFXUHFRPPXQLFDWLRQV
Key = 7 Plain = ETARVQITCRJAKUPGGFGFHQTUGEWTGEQOOWPKECVKQPU
Key = 8 Plain = DSZQUPHSBQIZJTOFFEFEGPSTFDVSFDPNNVOJDBUJPOT
Key = 9 Plain = CRYPTOGRAPHYISNEEDEDFORSECURECOMMUNICATIONS
Key = 10 Plain = BQXOSNFQZOGXHRMDDCDCENQRDBTQDBNLLTMHBZSHNMR
Key = 11 Plain = APWNRMEPYNFWGQLCCBCBDMPQCASPCAMKKSLGAYRGMLQ
Key = 12 Plain = ZOVMQLDOXMEVFPKBBABACLOPBZROBZLJJRKFZXQFLKP
```

- .
-

Substitution cipher - example

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
U	D	M	I	P	Y	Æ	K	O	X	S	N	Å	F	A

p	q	r	s	t	u	v	w	x	y	z	æ	ø	å
E	R	T	Z	B	Ø	C	Q	G	W	H	L	V	J

Plaintext: fermatssisteteorem

Ciphertext: YPTÅUBZZOZBPBPATPÅ

What is the size of the key space?

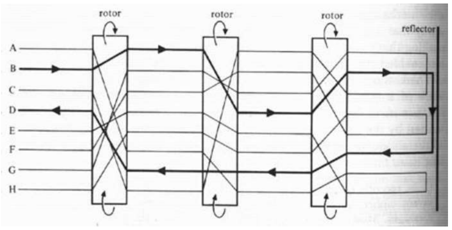
$884176199373970195454361600000 \approx 2^{103}$

Lessons learned

- A cipher with a small keyspace can easily be attacked by *exhaustive search*
- A *large keyspace* is necessary for a secure cipher, but it is by itself not suffcient
- Monoalphabetical substitution ciphers can easily be broken

Enigma

- German WW II crypto machine
- Many different variants
- Polyalphabetical substitution
- Analysed by Polish and English mathematicians




(c) 1995, Morton Swimmer

Enigma key list

Geheim! Sonder - Maschinenschlüssel BGT

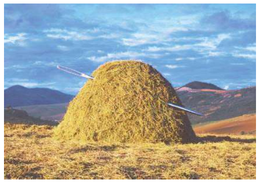
Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT IW SK UY DF GV LJ BO MX	vyj
30.	III V II	Y V P	OR KI JV CH ZK MU BF YC DS GP	cqr
29.	V IV I	O H R	UX JC PB LK TA ED ST DS LU FI	vhf

Practical complexity for attacking Enigma

Cryptoanalytical assumptions during WW II:

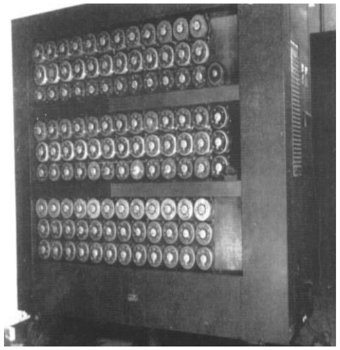
- 3 out of 5 rotors with known wiring
- 10 stecker couplings
- Known reflector

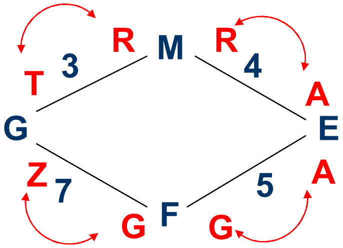
N = 150 738 274 937 250 · 60 · 17 576 · 676 = 107458687327250619360000 (77 bits)



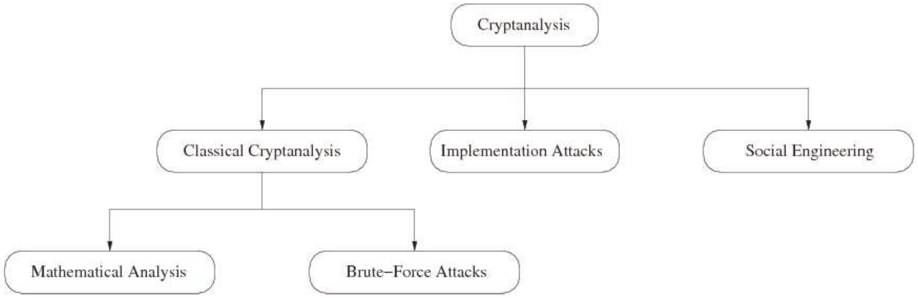
Attacking ENIGMA

Posisjon:	1	2	3	4	5	6	7
Chiffertekst:	J	T	G	E	F	P	G
Crib:	R	O	M	M	E	L	F





Cryptanalysis: Attacking Cryptosystems



- **Classical Attacks**
  - Mathematical Analysis
  - Brute-Force Attack
- **Implementation Attack**: Try to extract the key through reverse engineering or power measurement, e.g., for a banking smart card.
- **Social Engineering**: E.g., trick a user into giving up her password

---

Brute-Force Attack (or Exhaustive Key Search)

- Treats the cipher as a black box
- Requires (at least) 1 plaintext-ciphertext pair (x_0, y_0)
- Check all possible keys until condition is fulfilled:

$$d_K(y_0) = x_0$$

- How many keys to we need ?

Key length in bit	Key space	Security life time (assuming brute-force as best possible attack)
64	2^{64}	**Short term** (few days or less)
128	2^{128}	**Long-term** (several decades in the absence of quantum computers)
256	2^{256}	**Long-term** (also resistant against quantum computers – note that QC do not exist at the moment and might never exist)

Attack models:

Known ciphertext

Known plaintext

Chosen plaintext (adaptive)

Chosen ciphertext (adaptive)

What are the goals of the attacker?

- Find the secret plaintext or part of the plaintext
- Find the encryption key
- Distinguish the encryption of two different plaintexts

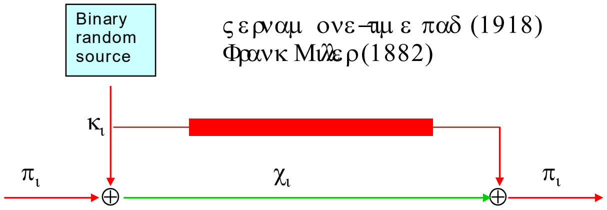
How clever is the attacker?

Does secure ciphers exist?

- What is a secure cipher?
  - Perfect security
  - Computational security
  - Provable security

"I'm sorry, we already have a director of security..."

A perfect secure crypto system



ςερναμ ονε-τιμε παδ (1918)
Φρανκ Μιλλερ (1882)

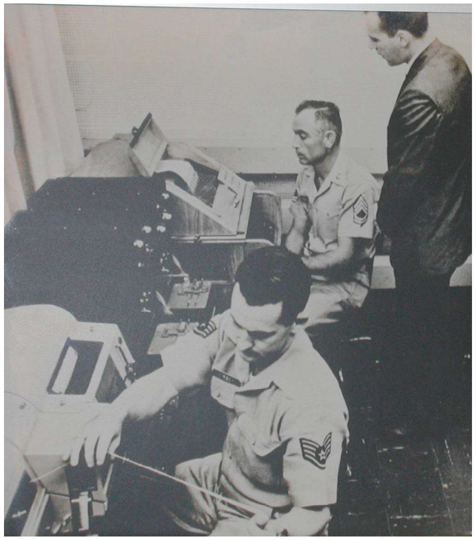
$\chi_\iota = \pi_\iota \oplus \kappa_\iota$
$\pi_\iota = \chi_\iota \oplus \kappa_\iota = \pi_\iota \oplus \kappa_\iota \oplus \kappa_\iota = \pi_\iota$
Νοτε: $\alpha \oplus \beta = \alpha + \beta$ (μοδ 2)

Οφφερσ περφεχτ σεχυριτψ ασσυμινγ τηε κεψ ισ περφεχτλψ ρανδομ, οφ σαμε λενγτη ασ Τηε Μεσσαγε; ανδ ονλψ υσεδ ονχε. Προϖεδ βψ Χλαυδε Ε. Σηαννον ιν 1949.

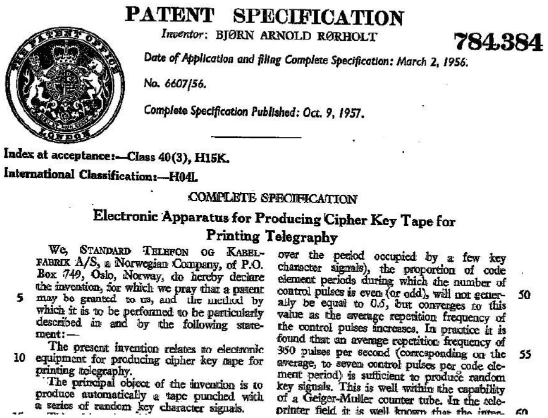
ETCRRM

- Electronic Teleprinter Cryptographic Regenerative Repeater Mixer (ETCRRM)
- Invented by the Norwegian Army Signal Corps in 1950
- Bjørn Rørholt, Kåre Mesingseth
- Produced by STK
- Used for ”Hot-line” between Moskva and Washington
- About 2000 devices produced

White House Crypto Room 1960s



Producing key tape for the one-time pad



PATENT SPECIFICATION

Inventor: BJØRN ARNOLD RØRHOLT

784,384

Date of Application and filing Complete Specification: March 2, 1956.

No. 6607/56.

Complete Specification Published: Oct. 9, 1957.

Index at acceptance:—Class 40(3), H15K.

International Classification:—H04L.

COMPLETE SPECIFICATION

Electronic Apparatus for Producing Cipher Key Tape for Printing Telegraphy

We, STANDARD TELEFON OG KABELFABRIK A/S, a Norwegian Company, of P.O. Box 749, Oslo, Norway, do hereby declare the invention, for which we pray that a patent may be granted to us, and the method by which it is to be performed to be particularly described in and by the following statement:—

The present invention relates to electronic equipment for producing cipher key tape for printing telegraphy.

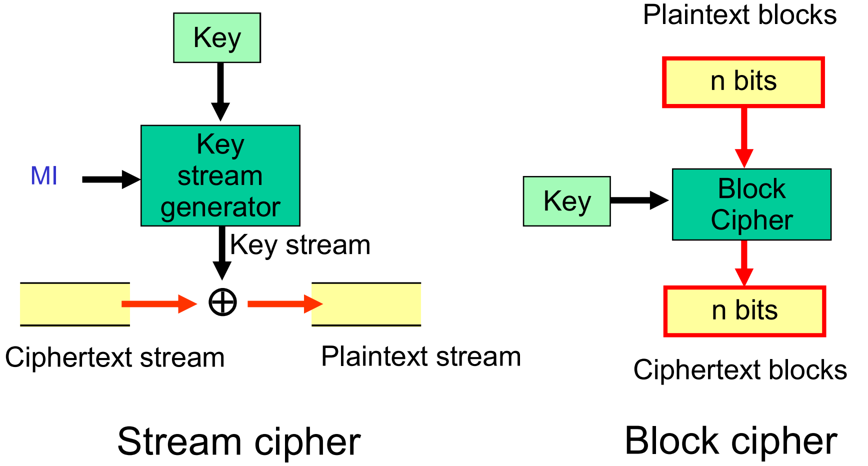
The principal object of the invention is to produce automatically a tape punched with a series of random key character signals.

over the period occupied by a few key character signals), the proportion of code element periods during which the number of control pulses is even (or odd), will not generally be equal to 0.5, but converges to this value as the average repetition frequency of the control pulses increases. In practice it is found that an average repetition frequency of 350 pulses per second (corresponding on the average, to seven control pulses per code element period) is sufficient to produce random key signals. This is well within the capability of a Geiger-Muller counter tube. In the teleprinter field it is well known that the inter-

Symmetric encryption

- Is it possible to design secure and practical crypto?

Stream Cipher vs. Block Cipher



Key

MI

Key stream generator

Key stream

⊕

Ciphertext stream

Plaintext stream

Stream cipher

Plaintext blocks

n bits

Key

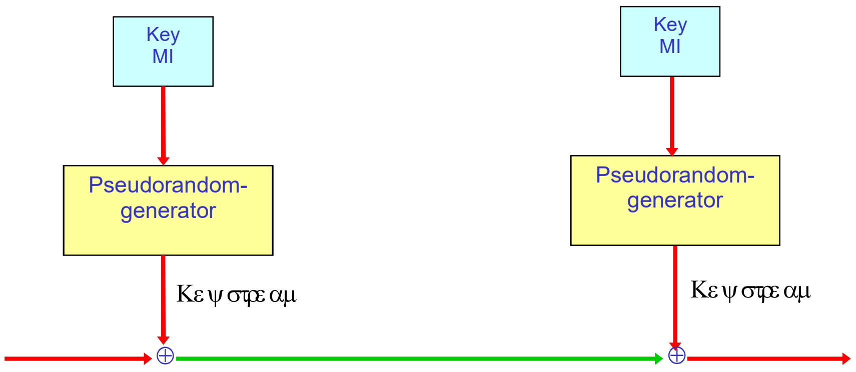
Block Cipher

n bits

Ciphertext blocks

Block cipher

Symmetric stream cipher



Key MI

Pseudorandom-generator

Κεψ στρεαμ

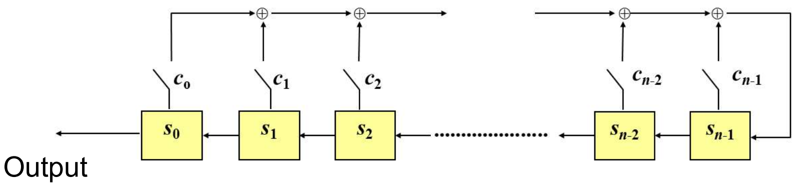
Key MI

Pseudorandom-generator

Κεψ στρεαμ

LFSR

Linear feedback shift register



Υσινγ n φλιπ-φλοπσ ωε μαψ γενερατε α βιναρψ σεθυενχε οφ περιοδ 2^n –1

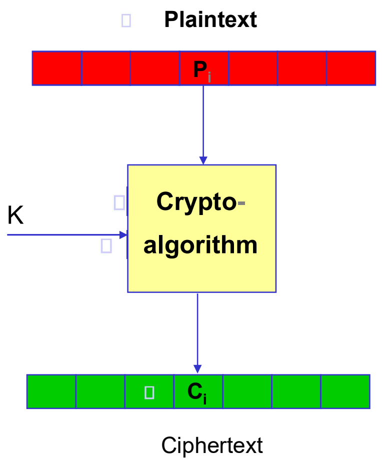
$$s_{n+i} = c_0\, s_i + c_1\, s_{i+1} + \cdots + c_{n-1}\, s_{i+n-1}$$

Note: The stream cipher is stateful

LFSR - properties

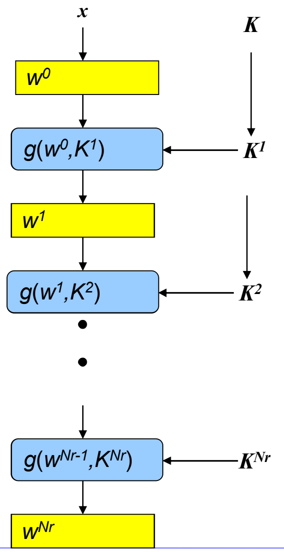
- Εασψ το ιμπλεμεντ ιν ΗΩ, οφφερσ φαστ χλοχκινγ
- Τηε ουτπυτ σεθυενχε ισ χομπλετελψ δετερμινεδ οφ τηε ινιτιαλ στατε ανδ τηε φεεδβαχκ χοεφφιχιεντσ
- Using “correct” feedback a register of length n μαψ γενερατε α σεθυενχε ωιτη περιοδ 2^n-1
- Τηε σεθυενχε ωιλλ προϖιδε γοοδ στατιστιχαλ προπερτιεσ
- Κνοωινγ 2n χονσεχυτιϖε βιτσ οφ τηε κεψστρεαμ, ωιλλ ρεϖεαλ τηε ινιτιαλ στατε ανδ φεεδβαχκ
- Τηε λινεαριτψ μεανσ τηατ α σινγλε ΛΦΣΡ ισ χομπλετελψ υσελεσσ ασ α στρεαμ χιπηερ, βυτ ΛΦΣΡσ μαψ βε α υσεφυλ βυιλδινγ βλοχκ φορ τηε δεσιγν οφ α στρονγ στρεαμ χιπηερ

Symmetric block cipher



- The algorithm represents a family of permutations of the message space
- Normally designed by iterating a less secure round function
- May be applied in different operational modes
- Must be impossible to derive K based on knowledge of P and C

Itrerated block cipher design



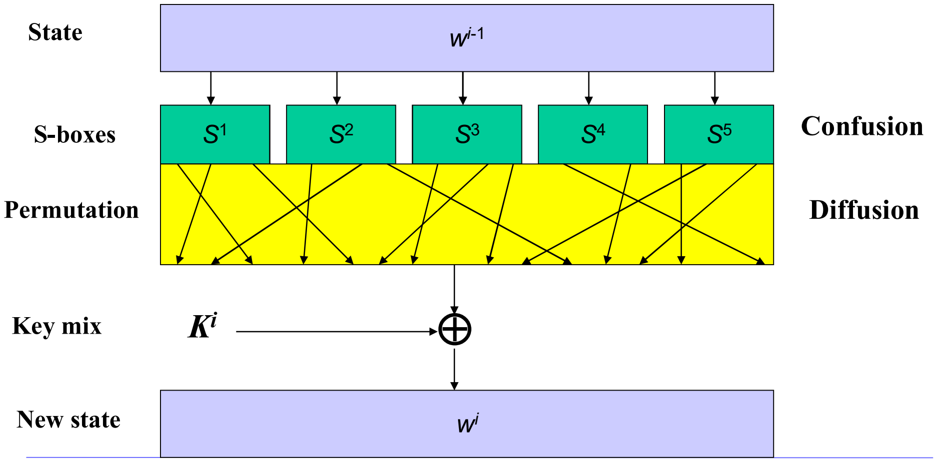
Algorithm:

```
$w^0 \leftarrow x$
$w^1 \leftarrow g(w^0,K^1)$
$w^2 \leftarrow g(w^1,K^2)$
•
•
$w^{Nr-1} \leftarrow g(w^{Nr-2},K^{Nr-1})$
$w^{Nr} \leftarrow g(w^{Nr-1},K^{Nr})$
$y \leftarrow w^{Nr}$
```

NB! For a fixed *K*, *g* must be injective in order to decrypt *y*

Substitution-Permutation network (SPN):

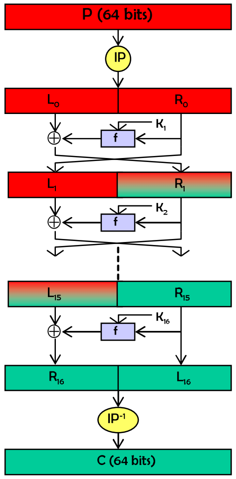
Round function *g* :



Data Encryption Standard

- Published in 1977 by the US National Bureau of Standards for use in unclassified government applications with a 15 year life time.
- 16 round Feistel cipher with 64-bit data blocks, 56-bit keys.
- 56-bit keys were controversial in 1977; today, exhaustive search on 56-bit keys is very feasible.
- Controversial because of classified design criteria, however no loop hole was ever found.

DES architecture

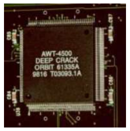


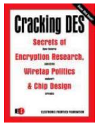
DES(P):
$(L_0, R_0) = IP(P)$
FOR i = 1 TO 16
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
$C = IP^{-1}(R_{16}, L_{16})$

64 bit data block
56 bit key
72.057.594.037.927.936

EFF DES-cracker

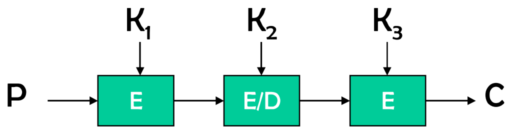
- Dedicated ASIC with 24 DES search engines
- 27 PCBs housing 1800 circuits
- Can test 92 billion keys per second
- Cost 250 000 $
- DES key found July 1998 after 56 hours search
- Combined effort DES Cracker and 100.000 PCs could test 245 billion keys per second and found key after 22 hours



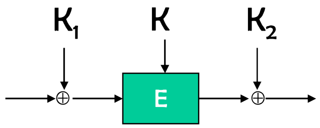


DES Status

- DES is the “work horse” which over 30 years have inspired cryptographic research and development
- “Outdated by now”!
- Single DES can not be considered as a secure block cipher
- Use 3DES (ANSI 9.52) or DESX



3DES

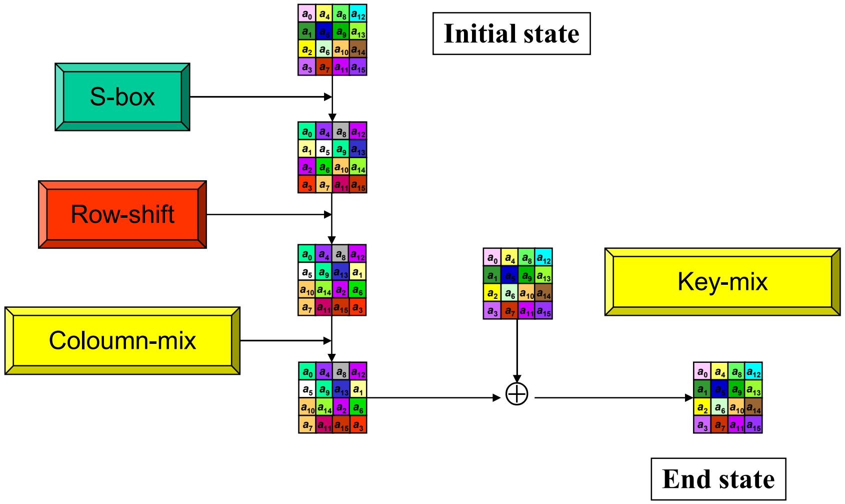


DESX

Advanced Encryption Standard

- Public competition to replace DES: because 56-bit keys and 64-bit data blocks no longer adequate.
- Rijndael nominated as the new Advanced Encryption Standard (AES) in 2001 [FIPS-197].
- Rijndael (pronounce as “Rhine-doll”) designed by Vincent Rijmen and Joan Daemen.
- 128-bit block size (Note error in Harris p. 809)
- 128-bit, 196-bit, and 256-bit key sizes.
- Rijndael is <u>not</u> a Feistel cipher.

Rijndael round function



Rijndael encryption

1. Key mix (round key K_0)
2. N_r-1 rounds containing:
    a) Byte substitution
    b) Row shift
    c) Coloumn mix
    d) Key mix (round key K_i)
3. Last round containing:
    a) Byte substitution
    b) Row shift
    c) Key mix (round key K_{Nr})

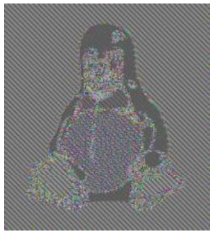
Key	Rounds
128	10
192	12
256	14

Block Ciphers: Modes of Operation

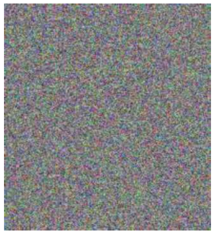
- Block ciphers can be used in different modes in order to provide different security services.
- Common modes include:
    - **E**lectronic **C**ode **B**ook (ECB)
    - **C**ipher **B**lock **C**haining (CBC)
    - **O**utput **F**eed**b**ack (OFB)
    - **C**ipher **F**eed**b**ack (CFB)
    - **C**oun**t**e**r** Mode (CTR)
    - **G**alois **C**ounter **M**ode (GCM) {Authenticated encryption}

Use a secure mode!

Plaintext



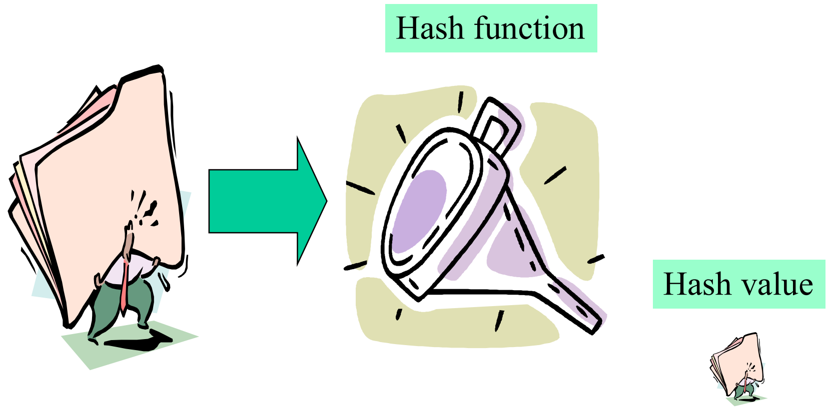
Ciphertext using
ECB mode



Ciphertext using
secure mode

Integrity Check Functions

Hash functions



Applications of hash functions

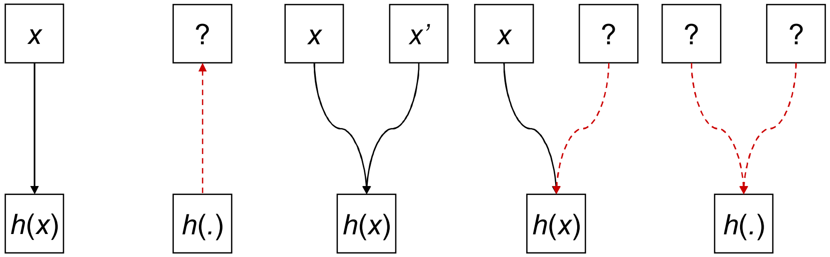
- Protection of password
- Comparing files
- Authentication of SW distributions
- Bitcoin
- Generation of Message Authentication Codes (MAC)
- Digital signatures
- Pseudo number generation/Mask generation functions
- Key derivation

Hash functions (message digest functions)

Requirements for a one-way hash function h:

1. Ease of computation: given x, it is easy to compute $h(x)$.
2. Compression: h maps inputs x of arbitrary bitlength to outputs $h(x)$ of a fixed bitlength n.
3. One-way: given a value y, it is computationally infeasible to find an input x so that $h(x)=y$.
4. Collision resistance: it is computationally infeasible to find x and x', where $x \neq x'$, with $h(x)=h(x')$ (note: two variants of this property).

Properties of hash functions



Ease of computation

Pre-image resistance

Collision

Weak collision resistance (2nd pre-image resistance)

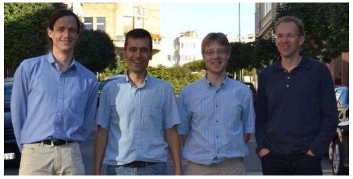
Strong collision resistance

Frequently used hash functions

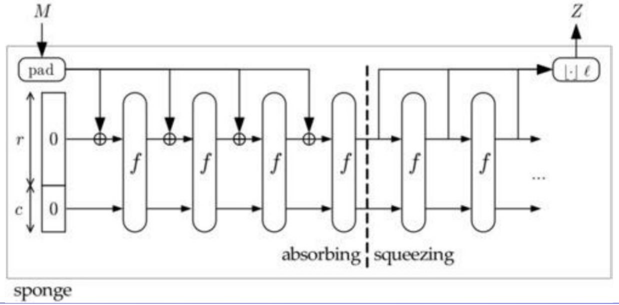
- MD5: 128 bit digest. Broken. Often used in Internet protocols but no longer recommended.
- SHA-1 (Secure Hash Algorithm):160 bit digest. Potential attacks exist. Designed to operate with the US Digital Signature Standard (DSA);
- SHA-256, 384, 512 bit digest. Still secure. Replacement for SHA-1
- RIPEMD-160: 160 bit digest. Still secure. Hash function frequently used by European cryptographic service providers.
- NIST competition for new secure hash algorithm, closed in 2012 with the winner:

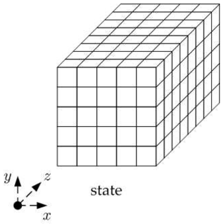
And the winner is?

- NIST announced Keccak as the winner of the SHA-3 Cryptographic Hash Algorithm Competition on October 2, 2012, and ended the five-year competition.
- Keccak was designed by a team of cryptographers from Belgium and Italy, they are:
  - Guido Bertoni (Italy) of STMicroelectronics,
  - Joan Daemen (Belgium) of STMicroelectronics,
  - Michaël Peeters (Belgium) of NXP Semiconductors, and
  - Gilles Van Assche (Belgium) of STMicroelectronics.



Keccak and sponge functions

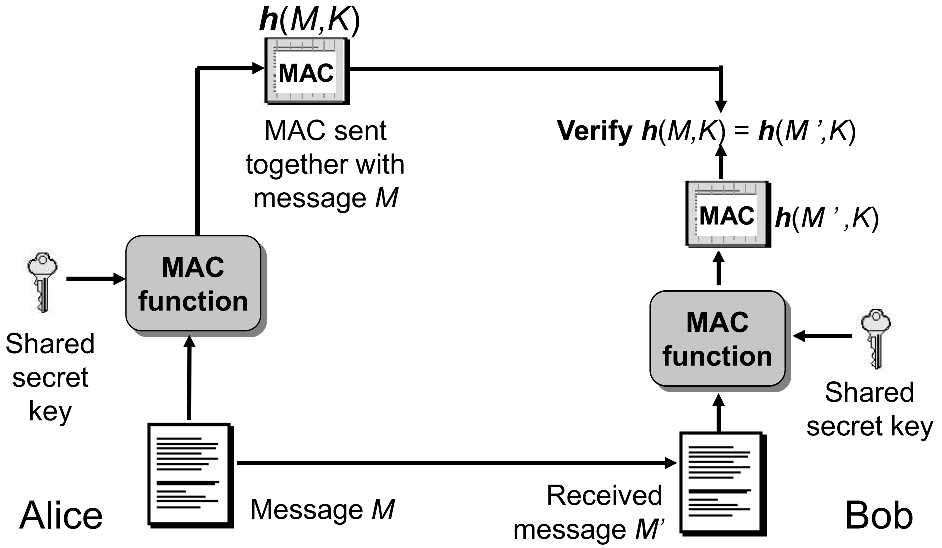




MAC and MAC algorithms

- MAC means two things:
  1. The computed message authentication code $h(M, k)$
  2. General name for algorithms used to compute a MAC
- In practice, the MAC algorithm is e.g.
  - HMAC (Hash-based MAC algorithm))
  - CBC-MAC (CBC based MAC algorithm)
  - CMAC (Cipher-based MAC algorithm)
- MAC algorithms, a.k.a. keyed hash functions, support data origin authentication services.

Practical message integrity with MAC



$\boldsymbol{h}(M,K)$

MAC

MAC sent together with message *M*

Verify $\boldsymbol{h}(M,K) = \boldsymbol{h}(M',K)$

MAC $\boldsymbol{h}(M',K)$

MAC function

MAC function

Shared secret key

Shared secret key

Alice

Message *M*

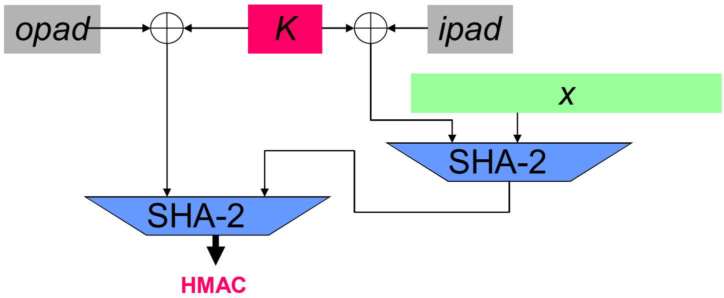
Received message *M'*

Bob

HMAC

- Define: *ipad* = 3636….36 (512 bit)
- *opad* = 5C5C…5C (512 bit)

- $\text{HMAC}_K(x) = \text{SHA-1}((K \oplus opad) \,||\, \text{SHA-1}((K \oplus ipad) \,||\, x))$



opad

K

ipad

x

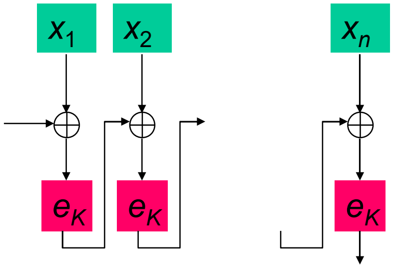
SHA-2

SHA-2

HMAC

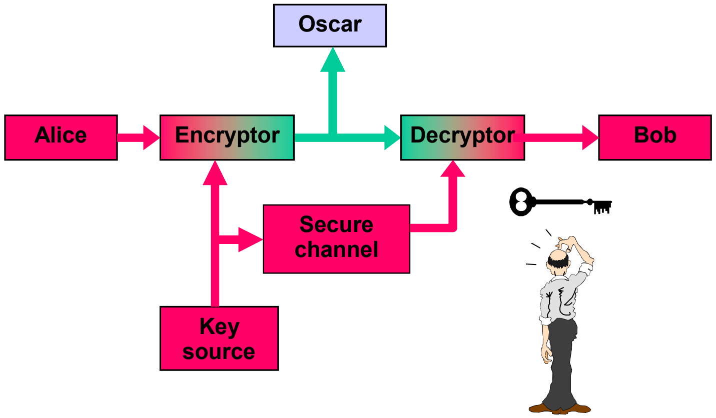
CBC-MAC

```
**CBC-MAC($x$, $K$)**
set $x = x_1 \| x_2 \| \dots \| x_n$
IV $\leftarrow$ 00 … 0
$y_0 \leftarrow$ IV
for $i \leftarrow 1$ to $n$
    do $y_i \leftarrow e_K(y_{i-1} \oplus x_i)$
return ($y_n$)
```



Public-Key Cryptography

Symmetric cryptosystem



Oscar

Alice

Encryptor

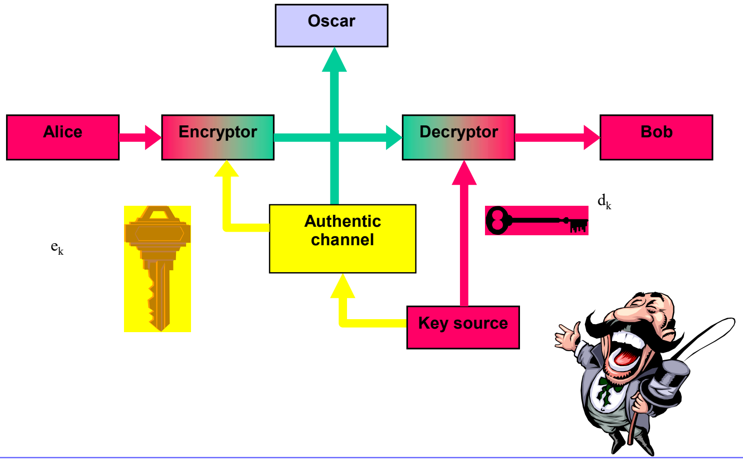
Decryptor

Bob

Secure channel

Key source

Asymmetric crypto system



Oscar

Alice

Encryptor

Decryptor

Bob

Authentic channel

Key source

e_k

d_k

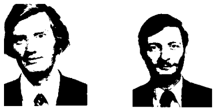
Public key inventors?

Marty Hellman and Whit Diffie, Stanford 1976

R. Rivest, A. Shamir and L. Adleman, MIT 1978

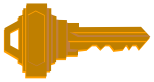
James Ellis, CESG 1970

C. Cocks, M. Williamson, CESG 1973-1974

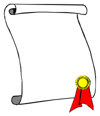


Asymmetric crypto

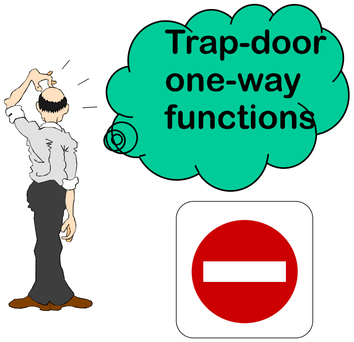
Public key **cryptography** was born in May 1975, the child of two problems and a misunderstanding!



Key Distribution!



Digital signing!



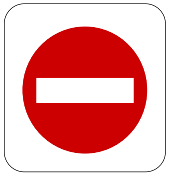
One-way functions

Modular power function

Given $n = pq$, where p and q are prime numbers. No efficient algoritms to find p and q.

Chose a positive integer b and define $f : Z_n \rightarrow Z_n$

$f(x) = x^b \bmod n$



Modular exponentiation

Given prime p, generator g and a modular power $a = g^x \pmod{p}$. No efficient algoritms to find x. $f : Z_p \rightarrow Z_p$

$f(x) = g^x \bmod p$

Diffie-Hellman key agreement (key exchange)

(provides no authentication)

Alice picks random integer a

$g^a \bmod p$ →

← $g^b \bmod p$

Computationally impossible to compute discrete logarithm

Bob picks random integer b

Alice computes the shared secret

$(g^b)^a = g^{ab} \bmod p$

Bob computes the same secret

$(g^a)^b = g^{ab} \bmod p$.

Example

- Z_{11} using $g = 2$:
  - $2^1 = 2$ (mod 11) $2^6 = 9$ (mod 11)
  - $2^2 = 4$ (mod 11) $2^7 = 7$ (mod 11)
  - $2^3 = 8$ (mod 11) $2^8 = 3$ (mod 11)
  - $2^4 = 5$ (mod 11) $2^9 = 6$ (mod 11)
  - $2^5 = 10$ (mod 11) $2^{10} = 1$ (mod 11)

- $\log_2 5 = 4$
- $\log_2 7 = 7$
- $\log_2 1 = 10$ ($\equiv$ 0 mod 10)

Example (2)

p =
3019662633453665226674644411185277127204721722044543980521881984280643980698016315342127777985323
7655786915947633907457862442472144616346714598423225826077976000905549946633556169688641786953396
0040623713995997295449774004045416733136225768251717475634638402409117911722715606961870076297223
4159137526583857970362142317237148068590959528891803802119028293828368386437223302582405986762635
8694772029533769528178666567879514981999272674689885986300092124730492599541021908208672727813714
8522572014844749083522090193190746907275606521624184144352256368927493398678089550310568789287558
75522700141844883356351776833964003

g =
1721484410294542720413651217788953849637988183467987659847411571496616170507302662812929883501017
4348250308006877834103702727269721499966768323290540216992770986728538508742382941595672248624817
9949179397494476750553747868409726540440305778460006450549504248776668609868201521098873552043631
7965394509849072406890541468179263651065250794610243485216627272170663501147422628994581789339082
7991578201408649196984764863302981052471409215846871176739109049866118609117954454512573209668379
5760420560620966283259002319100903253019113331521813948039086102149370446134117406508009893347295
86051242347771056691010439032429058

Finn *a* når

g^a (mod p) =
4411321635506521515968448863968324914909246042765028824594289876687657182492169027666262097915382
0952830455103982849705054980427000258241321067445164291945709875449674237106754516103276658256727
2413603372376920980338976048557155564281928533840136742732489850550648761094630053148353906425838
5317698361559907392252360968934338558269603389519179121915049733353702083721856421988041492207985
6566434665604898681669845852964624047443239120501341277499692338517113201830210812184500672101247
2700988032756016626566167579963223042395414267579262222147625965023052419869061244027798941410432
6855174387813098860607831088110617

Solution

a =

71893136149709653804503478677866573695060790720621260648699193249561437588126371185
81694154929099396752251787268346548051895320171079663652680741564200286881487888963
19895353311170236034836658449187117723820644855184055305945501710227615558093657781
93109639893698220411548578601884177129022057550866690223052160523604836233675971504
25938247630127368253363295292024736143937779912318142315499711747531882501424082252
28164641111954587558230112140813226698098654739025636607106425212812421038155501562
37005192231836155067262308141154795194735834753570104459663325337960304941906119476
18181858300094662765895526963615406

It is easy to compute g^a (mod p) {0.016 s}, but it is computaionally infeasable to compute the exponent *a* from the g^a.

Diffie-Hellman Applications

- IPSec (IP Security)
  - IKE (Internet Key Exchange) is part of the IPSec protocol suite
  - IKE is based on Diffie-Hellman Key Agreement
- SSL/TLS
  - Several variations of SSL/TLS protocol including
    - Fixed Diffie-Hellman
    - Ephemeral Diffie-Hellman
    - Anonymous Diffie-Hellman

Ron Rivest, Adi Shamir and Len Adleman

- Read about public-key cryptography in 1976 article by Diffie & Hellman: *"New directions in cryptography"*
- Intrigued, they worked on finding a practical algorithm
- Spent several months in 1976 to re-invent the method for non-secret/public-key encryption discovered by Clifford Cocks 3 years earlier
- Named RSA algorithm

RSA parametre (textbook version)

- Bob generates two large prime numbers p and q and computes $n = p \cdot q$.
- He then computes a public encryption exponent e, such that
- $(e, (p-1)(q-1)) = 1$ and computes the corresponding decryption exsponent d, by solving:

$$d \cdot e \equiv 1 \pmod{(p-1)(q-1)}$$

- Bob's public key is the pair $P_B = (e, n)$ and the corresponding private and secret key is $S_B = (d, n)$.

Encryption: $C = M^e \pmod{n}$

Decryption: $M = C^d \pmod{n}$

RSA toy example

- Set $p = 157$, $q = 223$. Then $n = p \cdot q = 157 \cdot 223 = 35011$ and $(p-1)(q-1) = 156 \cdot 222 = 34632$
- Set encryption exponent: $e = 14213$ {gcd(34632,14213) = 1}
- Public key: (14213, 35011)
- Compute: $d = e^{-1} = 14213^{-1} \pmod{34632} = 31613$
- Private key: (31613, 35011)

- <u>Encryption:</u>
- Plaintext M = 19726, then $C = 19726^{14213} \pmod{35011} = 32986$

- <u>Decryption:</u>
- Ciphertext C = 32986, then $M = 32986^{31613} \pmod{35011} = 19726$

Factoring record– December 2009

Find the product of

p = 33478071698956898786044169848212690817704794983713768568
912431388982883793878002287614711652531743087737814467999489

and

q= 36746043666799590428244633799627952632279158164343087642676
032283815739666511279233373417143396810270092798736308917?

Answer:

n= 12301866845301177551304949583849627207728535695953347921973224521517264005072636575187452021997864693899564749427740638459251925573263034537315482685079170261221429134616704292143116022212404792747377940806653514195974598569021434 13

Computation time ca. 0.0000003 s on a fast laptop!
RSA768 - Largest RSA-modulus that have been factored (12/12-2009)
Up to 2007 there was 50 000$ prize money for this factorisation!

Computational effort?

- Factoring using NFS-algorithm (Number Field Sieve)
- 6 mnd using 80 cores to find suitable polynomial
- Solding from August 2007 to April 2009 (1500 AMD64-år)
- 192 796 550 * 192 795 550 matrise (105 GB)
- 119 days on 8 different clusters
- Corresponds to 2000 years processing on one single core 2.2GHz AMD Opteron (ca. 2^{67} instructions)

Asymmetric Ciphers: Examples of Cryptosystems

- RSA: best known asymmetric algorithm.
  - RSA = Rivest, Shamir, and Adleman (published 1977)
  - Historical Note: U.K. cryptographer Clifford Cocks invented the same algorithm in 1973, but didn't publish.
- ElGamal Cryptosystem
  - Based on the difficulty of solving the discrete log problem.
- Elliptic Curve Cryptography
  - Based on the difficulty of solving the EC discrete log problem.
  - Provides same level of security with smaller key sizes.

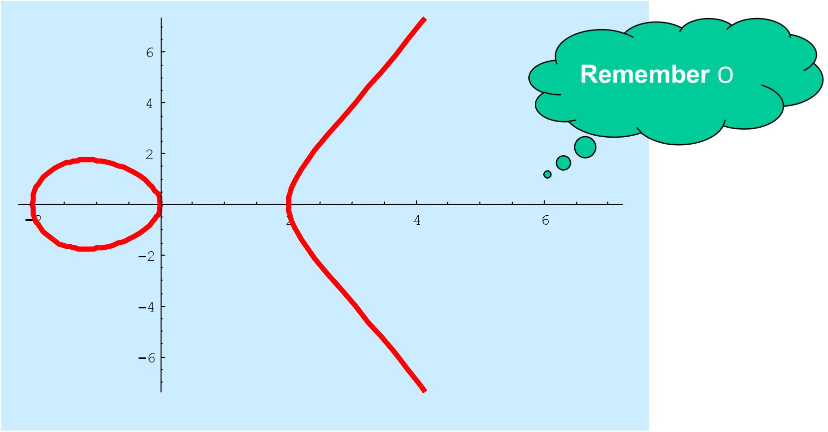
Elliptic curves

- Let $p > 3$ be a prime. An elliptic curve $y^2 = x^3 + ax + b$ over GF(p) = $\mathbb{Z}_p$ consist of all solutions $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ to the equation

$$\boxed{y^2 \equiv x^3 + ax + b \pmod{p}}$$

- where $a, b \in \mathbb{Z}_p$ are constants such that $4a^3 + 27b^2 \neq 0 \pmod{p}$, together with a special point $\mathcal{O}$ which is denoted as *the point at infinity*.

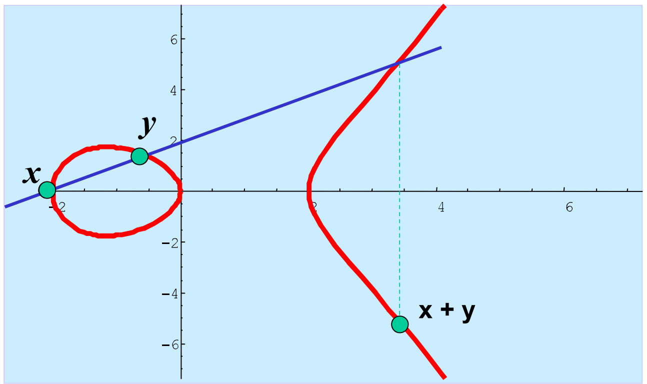
Elliptic curve over $\mathbb{R}$



Remember $\mathcal{O}$

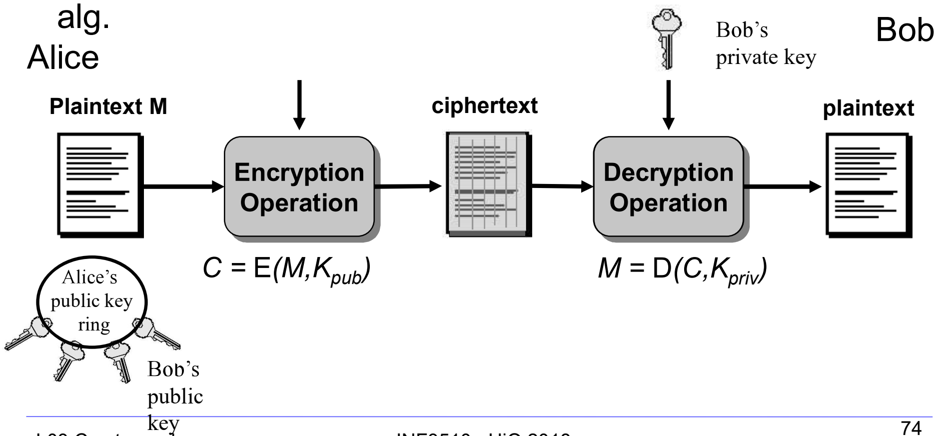
$y^2 = x^3 - 4x$

Point addition



Asymmetric Encryption: Basic encryption operation

- In practice, large messages are not encrypted directly with asymmetric algorithms. Hybrid systems are used, where only symmetric session key is encrypted with asymmetric alg.



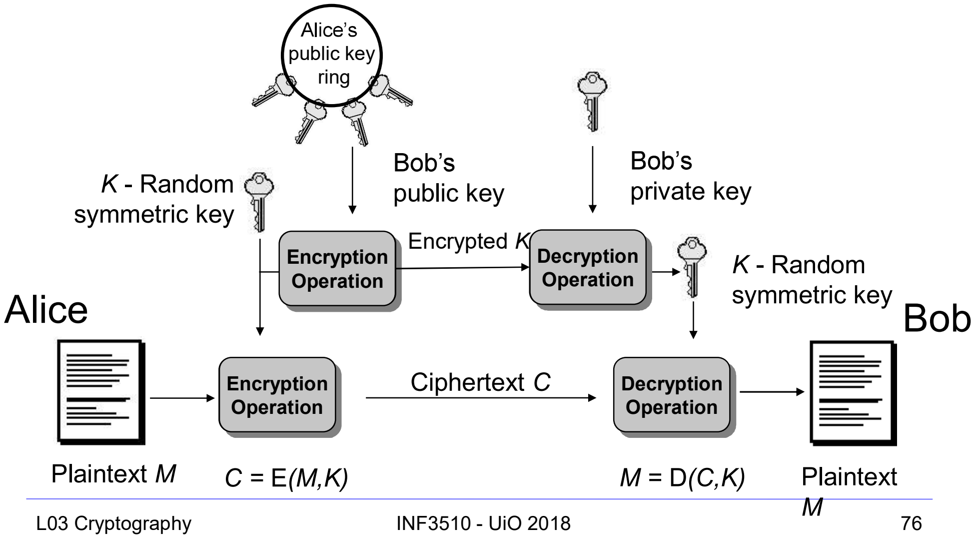
$C = E(M, K_{pub})$

$M = D(C, K_{priv})$

Hybrid Cryptosystems

- Symmetric ciphers are faster than asymmetric ciphers (because they are less computationally expensive), but ...
- Asymmetric ciphers simplify key distribution, therefore ...
- a combination of both symmetric and asymmetric ciphers can be used – a hybrid system:
  - The asymmetric cipher is used to distribute a randomly chosen symmetric key.
  - The symmetric cipher is used for encrypting bulk data.

Confidentiality Services: Hybrid Cryptosystems



$C = E(M, K)$

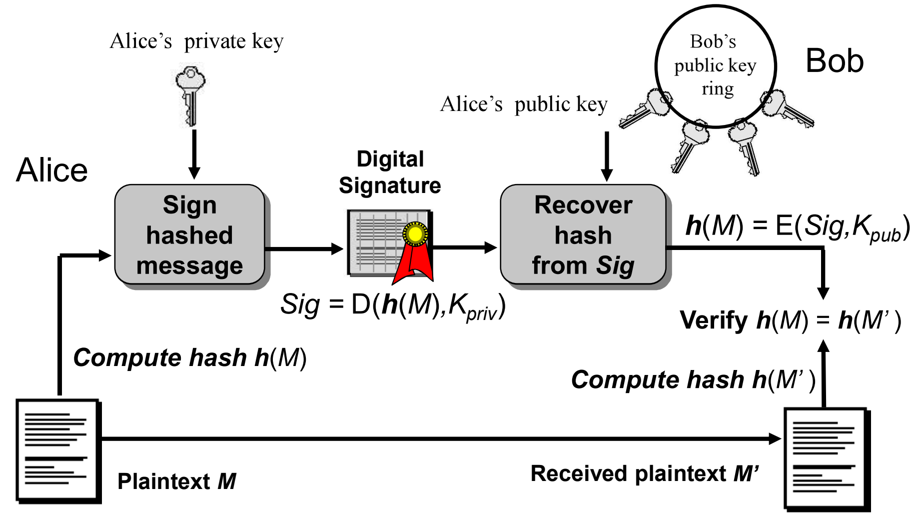
$M = D(C, K)$

Digital Signatures

Digital Signature Mechanisms

- A MAC cannot be used as evidence that should be verified by a third party.
- Digital signatures used for non-repudiation, data origin authentication and data integrity services, and in some authentication exchange mechanisms.
- Digital signature mechanisms have three components:
  - key generation
  - signing procedure (private)
  - verification procedure (public)
- Algorithms
  - RSA
  - DSA and ECDSA

Practical digital signature based on hash value



Digital Signatures

- To get an authentication service that links a document to *A*'s name (identity) and not just a verification key, we require a procedure for *B* to get an authentic copy of *A*'s public key.
- Only then do we have a service that proves the authenticity of documents 'signed by *A*'.
- This can be provided by a PKI (Public Key Infrastructure)
- Yet even such a service does not provide non-repudiation at the level of persons.

Difference between MACs & Dig. Sig.

- MACs and digital signatures are both authentication mechanisms.
- MAC: the verifier needs the secret that was used to compute the MAC; thus a MAC is unsuitable as evidence with a third party.
  - The third party does not have the secret.
  - The third party cannot distinguish between the parties knowing the secret.

- Digital signatures can be validated by third parties, and can in theory thereby support both non-repudiation and authentication.

Key length comparison:

Symmetric and Asymmetric ciphers offering comparable security

AES Key Size	RSA Key Size	Elliptic curve Key Size
-	1024	163
128	3072	256
192	7680	384
256	15360	512

Another look at key lengths

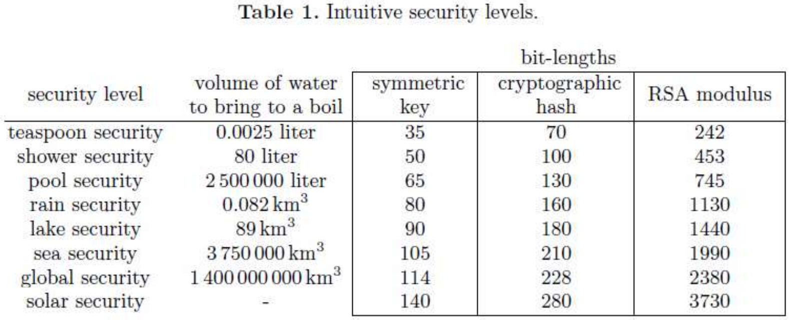


Table 1. Intuitive security levels.

		bit-lengths		
security level	volume of water to bring to a boil	symmetric key	cryptographic hash	RSA modulus
teaspoon security	0.0025 liter	35	70	242
shower security	80 liter	50	100	453
pool security	2 500 000 liter	65	130	745
rain security	$0.082\,\text{km}^3$	80	160	1130
lake security	$89\,\text{km}^3$	90	180	1440
sea security	$3\,750\,000\,\text{km}^3$	105	210	1990
global security	$1\,400\,000\,000\,\text{km}^3$	114	228	2380
solar security	-	140	280	3730

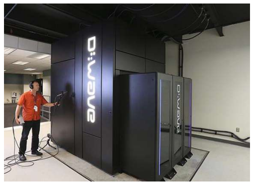
The eavesdropper strikes back!

Computing

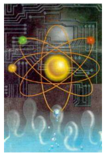
NSA Says It "Must Act Now" Against the Quantum Computing Threat

The National Security Agency is worried that quantum computers will neutralize our best encryption – but doesn't yet know what to do about that problem.

by Tom Simonite February 3, 2016



Quantum Computers



- Proposed by Richard Feynman 1982
- Boosted by P. Schor's algorithm for integer factorization and discrete logarithm in quantum polynomial time
- Operates on qubit – superposition of 0 and 1
- IBM built a 7-bit quantum computer and could find the factors of the integer 15 using NMR techniques in 2001
- NMR does not scale
- Progress continues, but nobody knows if or when a large scale quantum computer ever can be constructed
- QC will kill current public key techniques, but does not mean an end to symmetric crypto

---

Qubit (bra-ket notation)

A qubit is a unit vector in a two dimensional complex vector space with fixed basis. Orthonormal basis $|0\rangle$ and $|1\rangle$

may correspond $|\uparrow\rangle$ and $|\rightarrow\rangle$ (vertical or horizontal polarization)

The basis states $|0\rangle$ and $|1\rangle$ are taken to represent the classical bit values 0 and 1 respectively

Qubits can be in a superposition of $|0\rangle$ and $|1\rangle$ such as

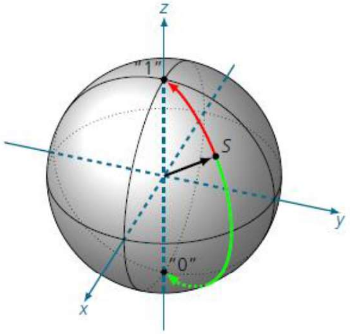
$$\boldsymbol{\Psi = \alpha |0\rangle + \beta |1\rangle}, \textbf{ where , } \boldsymbol{|\alpha|^2 + |\beta|^2 = 1}$$

Thus, $|\alpha|^2$ and $|\beta|^2$ are the probabilities that the measured value are $|0\rangle$ and $|1\rangle$ respectively

---

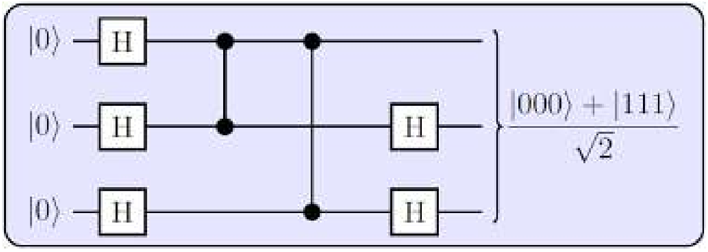
Classical bit vs. qubits

- ● 1
- ● 0

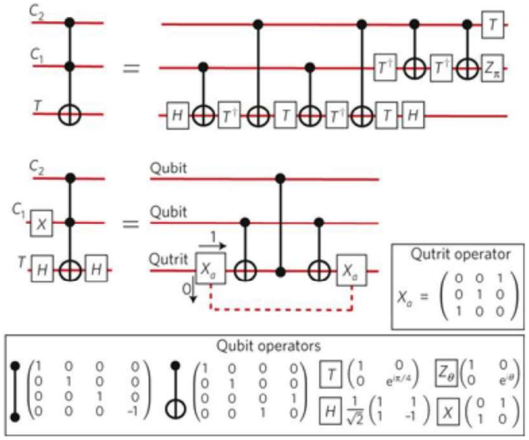


$$\boldsymbol{\Psi = \alpha |0\rangle + \beta |1\rangle}, \text{ where } \boldsymbol{|\alpha|^2 + |\beta|^2 = 1}$$

Operations on qubits

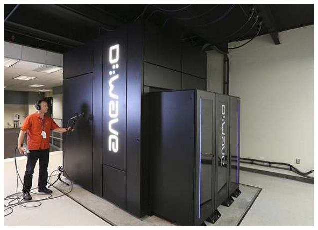


Quantum logic



QC impact to cryptography

- When will a quantum computer be built?
  - 15 years, $1 billion USD, nuclear power plant (PQCrypto 2014, Matteo Mariantoni)
- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~Elliptic Curve Cryptography (ECDSA)~~
    - ~~Finite Field Cryptography (DSA)~~
    - ~~Diffie-Hellman key exchange~~
  - Symmetric key crypto:
    - AES Need larger keys
    - Triple DES Need larger keys
  - Hash functions:
    - SHA-1, SHA-2 and SHA-3 Use longer output



Current world record of QF!

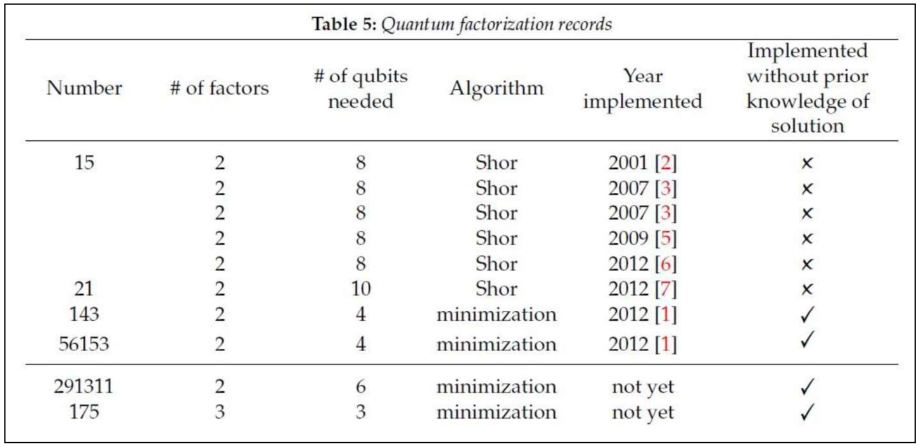


Table 5: *Quantum factorization records*

Number	# of factors	# of qubits needed	Algorithm	Year implemented	Implemented without prior knowledge of solution
15	2	8	Shor	2001 [2]	×
	2	8	Shor	2007 [3]	×
	2	8	Shor	2007 [3]	×
	2	8	Shor	2009 [5]	×
	2	8	Shor	2012 [6]	×
21	2	10	Shor	2012 [7]	×
143	2	4	minimization	2012 [1]	✓
56153	2	4	minimization	2012 [1]	✓
291311	2	6	minimization	not yet	✓
175	3	3	minimization	not yet	✓

Two variants of quantum safe crypto

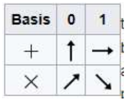
Quantum cryptography:

- The use of quantum mechanics to guarantee secure communication.
- It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages.

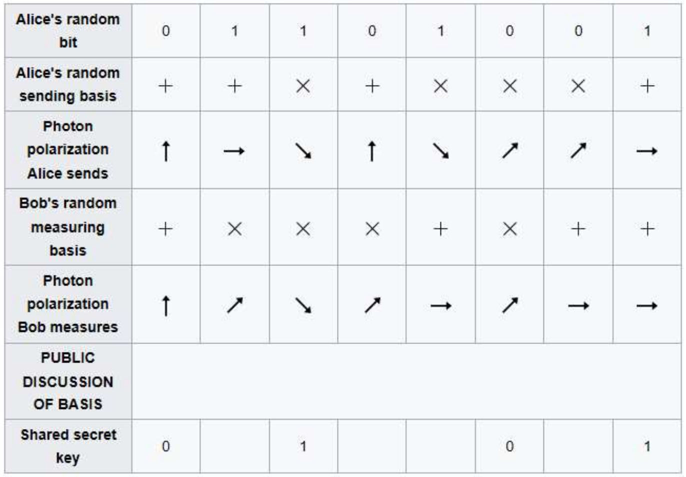
Quantum resistant cryptography:

- The use of cryptographic mechanisms based on computationally difficult problems for which no efficient quantum computing algorithm is known

Quantum Key Distribution



Basis	0	1
+	↑	→
×	↗	↘



Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

Quantum Resistant Cryptography

- Code Based Asymmetric Algorithms
- Lattice Based Asymmetric Algorithms
- Asymmetric Crypto based on Multivariate Polynomials
- Asymmetric Crypto based on Cryptographic Hash Functions
- Asymmetric Crypto based on Isogenies of (supersingular) elliptic curves

---

Follow Post Quantum crypto!

- https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography

Round 1 Submissions

Scientific America Technology, 10 Jan 2017

COMPUTING

Quantum Computers Ready to Leap Out of the Lab in 2017

Google, Microsoft and a host of labs and start-ups are racing to turn scientific curiosities into working machines

By Davide Castelvecchi, Nature magazine on January 4, 2017 Véalo en español

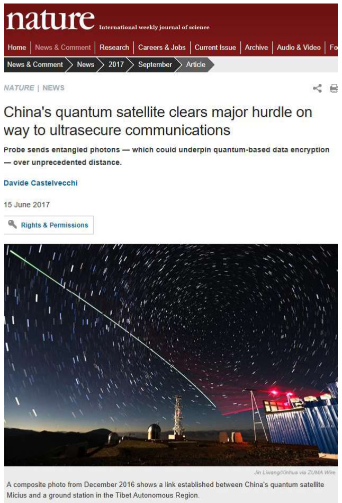
Credit: Mehau Kulyk Getty Images

Quantum computing has long seemed like one of those technologies that are 20 years away, and always will be. But 2017 could be the year that the field sheds its research-only image.

Computing giants Google and Microsoft recently hired a host of leading lights, and have set challenging goals for this year. Their ambition reflects a broader transition taking place at start-ups and academic research labs alike: to move from pure science towards engineering.

“People are really building things,” says Christopher Monroe, a physicist at the University of Maryland in College Park who co-founded the start-up IonQ in 2015. “I’ve never seen anything like that. It’s no longer just research.”

QKD via satellite



NATURE | NEWS

China's quantum satellite clears major hurdle on way to ultrasecure communications

Probe sends entangled photons — which could underpin quantum-based data encryption — over unprecedented distance.

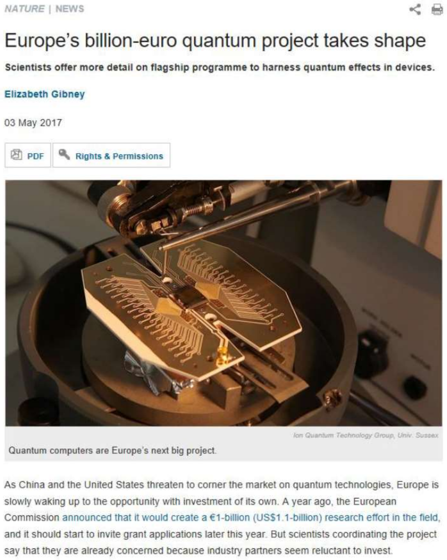
Davide Castelvecchi

15 June 2017

Jin Liwang/Xinhua via ZUMA Wire

A composite photo from December 2016 shows a link established between China's quantum satellite Micius and a ground station in the Tibet Autonomous Region.

More updates



NATURE | NEWS

Europe's billion-euro quantum project takes shape

Scientists offer more detail on flagship programme to harness quantum effects in devices.

Elizabeth Gibney

03 May 2017

Ion Quantum Technology Group, Univ. Sussex

Quantum computers are Europe's next big project.

As China and the United States threaten to corner the market on quantum technologies, Europe is slowly waking up to the opportunity with investment of its own. A year ago, the European Commission announced that it would create a €1-billion (US$1.1-billion) research effort in the field, and it should start to invite grant applications later this year. But scientists coordinating the project say that they are already concerned because industry partners seem reluctant to invest.

Update from two months ago

News room > News releases >

IBM Announces Advances to IBM Quantum Systems & Ecosystem

-- Client systems with 20 qubits ready for use; next-generation IBM Q system in development with first working 50 qubit processor
-- IBM expands its open-source quantum software package QISKit; offers the world's most advanced ecosystem for quantum computing

Select a topic or year

Yorktown Heights, N.Y. - 10 Nov 2017: IBM (NYSE: IBM) announced today two significant quantum processor upgrades for its IBM Q early-access commercial systems. These upgrades represent rapid advances in quantum hardware as IBM continues to drive progress across the entire quantum computing technology stack, with focus on systems, software, applications and enablement.

Swedish news from November

KVANTEDATAMASKIN

Svenske forskere får nær en milliard kroner til å utvikle kvantedatamaskin

AV: HARALD BROMBACH | MASKINVARE | PUBLISERT: 15. NOV. 2017 - 12:00

Med et budsjett på nærmere en milliard svenske kroner (omtrent 970 millioner NOK) skal prosessor Per Delsing ved Chalmers tekniska högskola i Gøteborg lede et initiativ som har som mål å utvikle en virkelig kraftig kvantedatamaskin.

– Målet vårt er å ha en fungerende kvantedatamaskin med minst hundre qubit. En slik datamaskin har mye større regnekraft enn de beste superdatamaskinene i dag og kan bli brukt til for eksempel å løse optimaliseringsproblemer, avansert maskinlæring og tunge beregninger av egenskapene til molekyler, sier Delsing i en pressemelding.

Andre områder hvor kvanteteknologien er aktuell, er innen kryptering og design av medisiner.

Les også: Intels nye brikke skal være et gjennombrudd innenfor kvantedatamaskiner

Minst 100 qubit

En qubit er i denne sammenheng en elektrisk mikrobrikke som tar vare på kvantetilstanden til ett enkelt foton. Mens 100 vanlig bit vanligvis er en ganske ubetydelig datamengde i dagens tradisjonelle datamaskiner, kan man i kvantedatamaskiner prosessere enorme datamengder selv med relativt få qubit.

IBM kunngjorde i forrige uke at selskapet har fått en prosessor med 50 qubit til å fungere, så 100 qubit er ikke til å kimse av, selv om det svenske prosjektet skal pågå i et tiår.

I likhet med blant annet IBM, skal den svenske forskningsgruppen benytte superledende kretser. Superledende qubit-er er noe forskere ved Chalmers har jobbet med i nærmere 20 år.

LES OGSÅ

Intels nye brikke skal være et gjennombrudd innenfor kvantedatamaskiner

Brave new crypto world…………….

Thank you!

End of lecture