

Chapter 2

Types of modern encryption

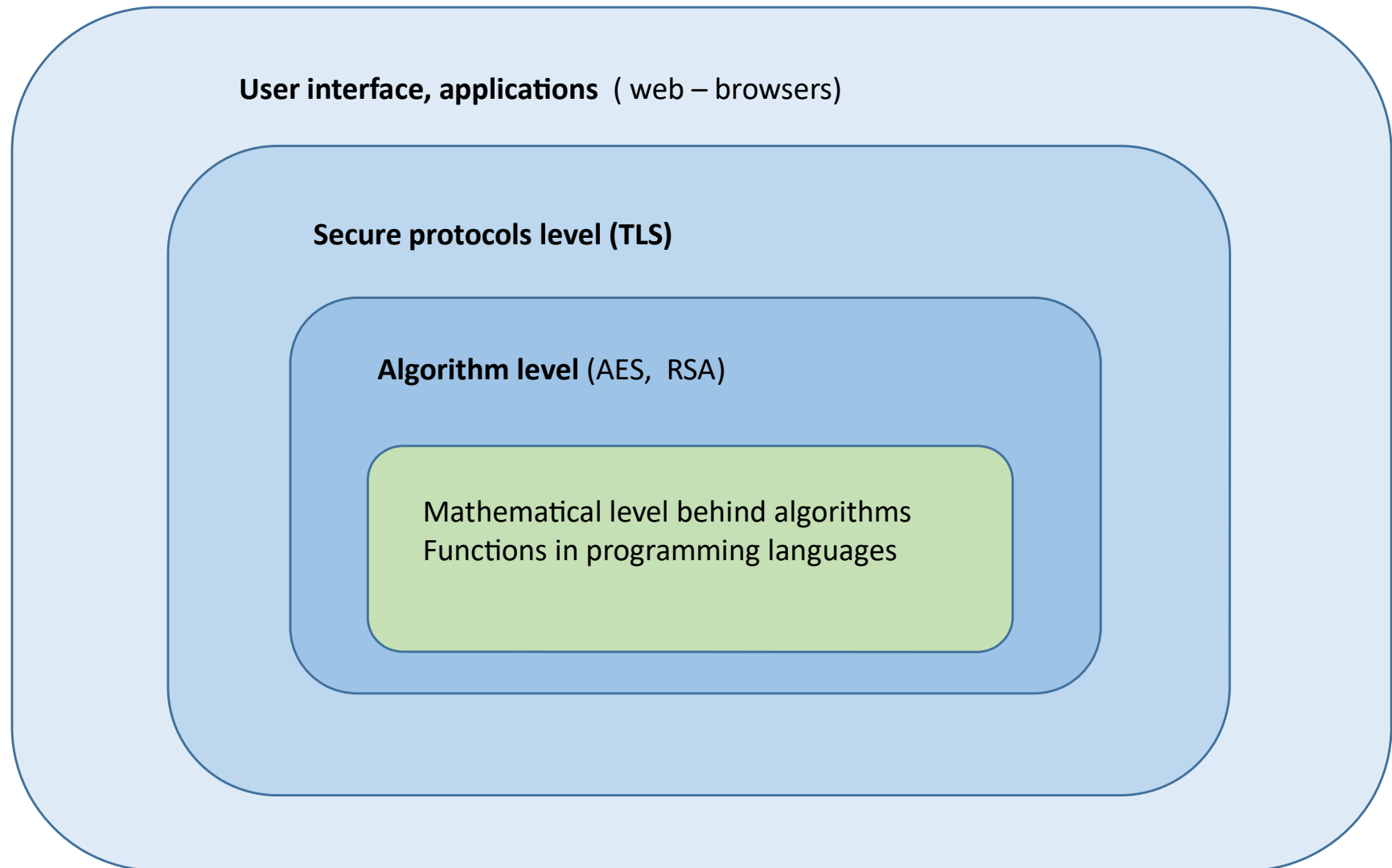
Secure connections viewed from different levels

- User interface, applications
- Secure protocols level
- Algorithm level
- Level of mathematical structures

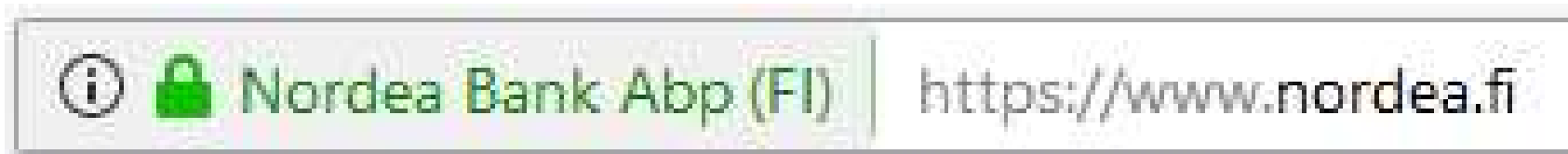
Block ciphers

Stream ciphers

Encryption at different levels



User level (browsers)



Users know that the connection is secure from the lock of URL row of the browser. If the lock is green, the connection is secure and encrypted and the server is authenticated. Red lock means possible security problems.

The encryption software which provides the secure connection is usually TLS.

Secure protocols level

In Mozilla Firefox browser clicking the lock reveals following information:

Tekniset tiedot

Yhteys salattu (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256-bittinen avain, TLS 1.2)

TLS ver 1.2 is a hybrid encryption software, which uses several algorithms for different functions. More than 95% of secure connections over Internet use TLS.

The basic functions of a hybrid encryption software are:

1. Authentication
2. Key exchange (agreeing of symmetric key)
3. Encryption of transmitted data
4. Digital signatures

Algorithmic level

Below list of algorithms is from Nordea Bank's TLS - connection

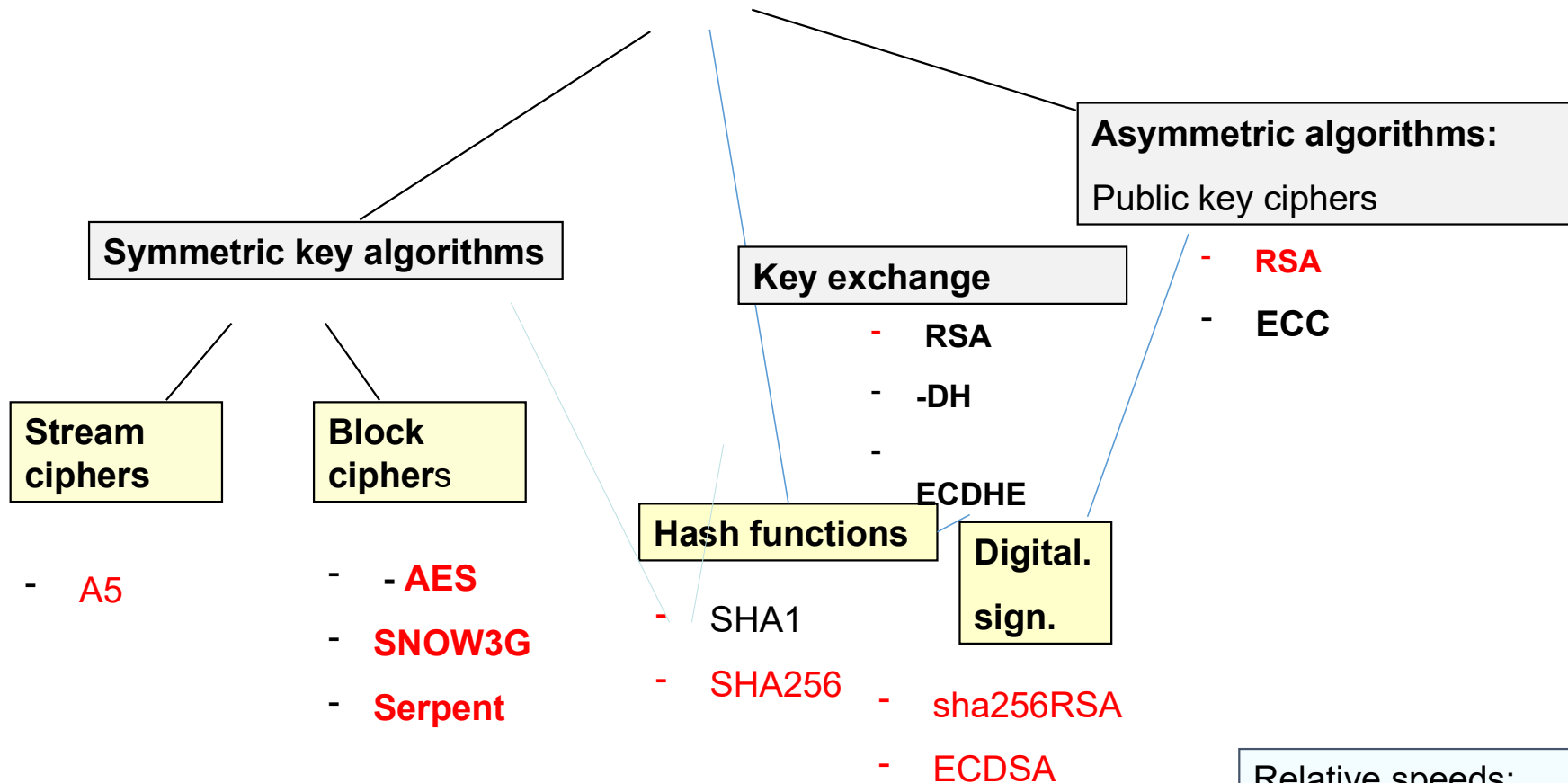
| Function | Algorithm name |
|--------------------------------|-------------------------|
| Server authentication | RSA |
| Key exchange | ECDHE |
| Encryption of transmitted data | AES256 GCM-moodi |
| Digital signature | sha384RSA |

4. Mathematical level

The algorithms of TLS and other modern software require lots of mathematics

- | | |
|---|--------------------------------|
| 1. Fermat's and Euler's theorems, Extended Euclid's algorithm | |
| 2. Random number generation | pseudorandomness |
| 3. Prime generation, tests | Fermat and Rabin- Miller tests |
| 4. Modular arithmetics | number sets Z_n |
| 5. Fast exponentiation mod n | Powermod - algorithm |
| 6. Inverses mod n | Euclid's extended algorithm |
| 7. Cyclic group Z_p^* | group theory |
| 8. Elliptic curves | group theory |

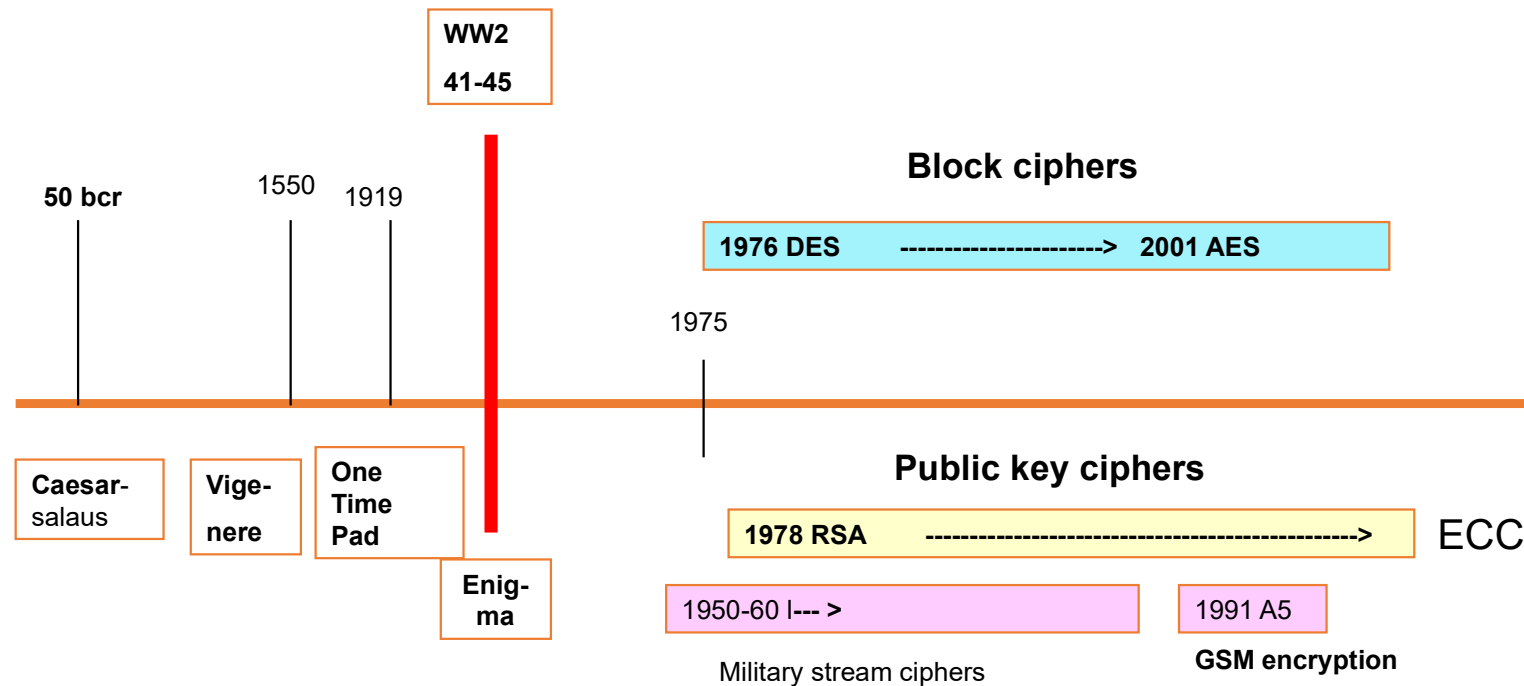
Algorithm types



Relative speeds:

| | |
|---------------|------|
| Hash | 3 |
| Stream cipher | 2 |
| Block cipher | 1 |
| Asymmetric | 0.02 |

Time line of encryption methods



Algorithms have long lifetime. RSA has been standard for 45 years in public key cryptography. Block cipher standard has changes only once during 45 years. Reasons for conservatism: 1. Changing algorithms costs money. 2. The security of algorithms are based on mathematical proofs, they have been tested for decennies.

Symmetric encryption algorithms

Classification

1. Block ciphers

- used both in wired and mobile communication
- Diffusion and confusion principles
- Permutation-substitution networks
- Modes of operation
- AES : block cipher standard

2. Synchronic stream ciphers

- no longer widely used
- GSM (G2)– encryption A5

Block ciphers

- Central part of secure connections. Block ciphers encrypt transmitted data reliably and effectively
- Provides fast symmetric encryption in which message is encrypted in blocks (size usually 128 bits)
- The present block cipher standard is AES (since 2001). It is used both in secure wired connections and in mobile networks

History of block ciphers

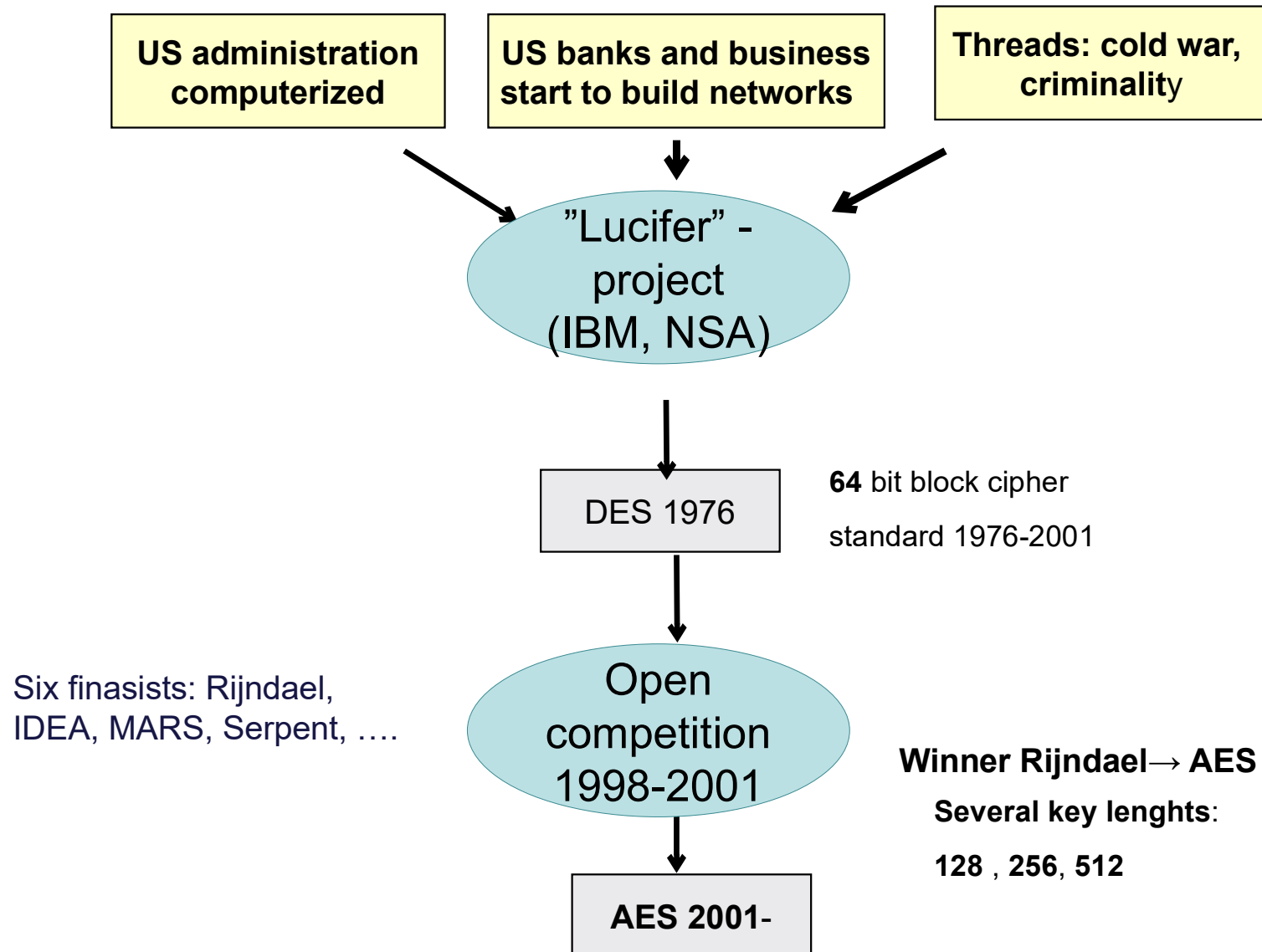
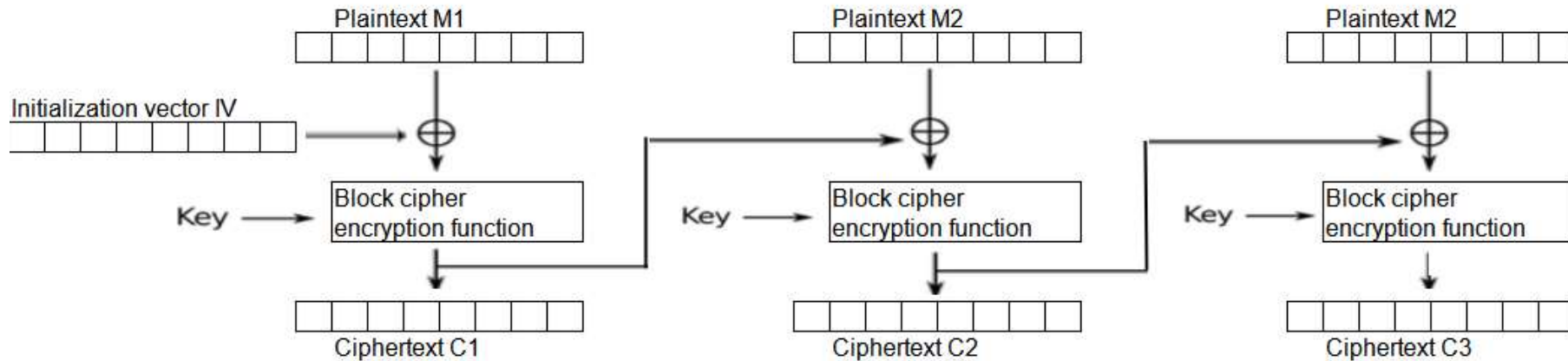


Diagram shows how block cipher works in CBC mode (CBC = cipher block chaining)



Principle:

Message m is divided into 128 bit blocks m_1, m_2, m_3, \dots

Key k has 128 bits in AES128. Cipher consists of blocks c_1, c_2, c_3, \dots

In CBC mode each output block is taken as 3rd input in calculation of next cipher block.

$$c_n = \text{AES}(m_n, k, c_{n-1})$$

Requirements for block ciphers

- Block cipher should have both software and hardware (chip) implementations (AES has both)
- Algorithm should be reliable and fast
- It can be applied to both data transfer and files
- Algorithm should be public and transparent (Kerckhoff principle)
- Key length should be at minimum 128 bits

Shannon's diffusion and confusion



The operation of block ciphers is based on two principles of Claude Shannon: diffusion and confusion

Diffusion: (dependence of cipher and message)

Changing one bit of message block should change in average half of the output bits. The output bits should equally depend on all input bits.

Confusion: (dependence of cipher and key)

Every bit of cipher should depend on all parts of the key. The change of one bit of the key, should change the output completely, not just part of it.

The ciphertext should be random and fulfill the properties of pseudorandom bit sequence (explained later)

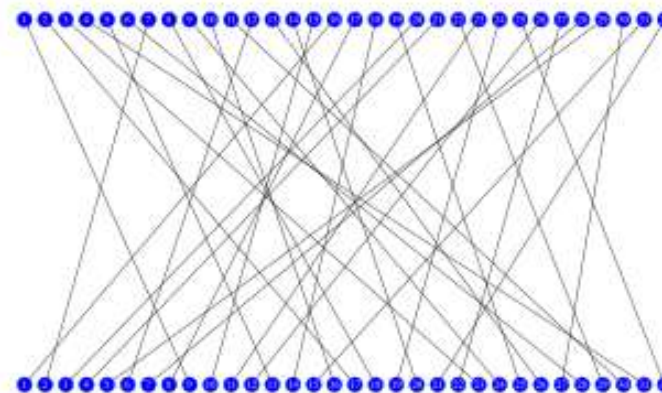
Permutation – Substitution networks

The principles of diffusion and confusion are usually implemented using a permutation - substitution network.

Substitution = replacing certain bit patterns with image patterns, traditionally using substitution tables called SBOX:es. Below a table of Sbox nr 6 of DES block cipher. In example bit sequence 011011 is mapped to 1001

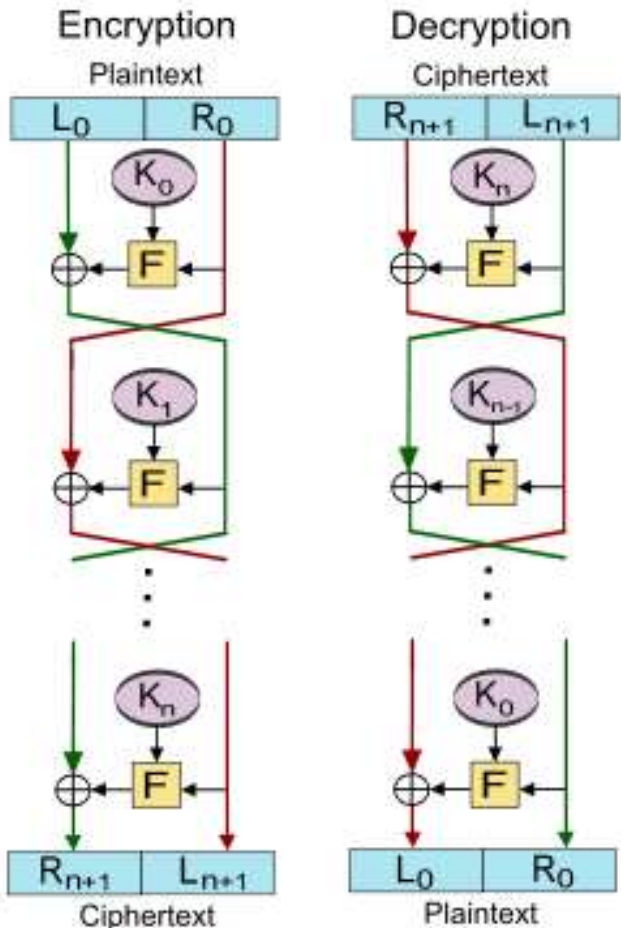
| S ₅ | | Middle 4 bits of input | | | | | | | | | | | | | | | |
|----------------|----|------------------------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| | | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |
| Outer bits | 00 | 0010 | 1100 | 0100 | 0001 | 0111 | 1010 | 1011 | 0110 | 1000 | 0101 | 0011 | 1111 | 1101 | 0000 | 1110 | 1001 |
| | 01 | 1110 | 1011 | 0010 | 1100 | 0100 | 0111 | 1101 | 0001 | 0101 | 0000 | 1111 | 1010 | 0011 | 1001 | 1000 | 0110 |
| | 10 | 0100 | 0010 | 0001 | 1011 | 1010 | 1101 | 0111 | 1000 | 1111 | 1001 | 1100 | 0101 | 0110 | 0011 | 0000 | 1110 |
| | 11 | 1011 | 1000 | 1100 | 0111 | 0001 | 1110 | 0010 | 1101 | 0110 | 1111 | 0000 | 1001 | 1010 | 0100 | 0101 | 0011 |

Permutation = reordering bits of a block using permutation tables. Figure shows how 64 bits are rearranged in P-box of DES block cipher.



Rounds: Permutation- Substitution loop runs several times, (f.e in DES algorithm 16 times) in order to remove all regularities in the cipher bit sequence.

Feistel network



IBM engineer Feistel created PS network in 1960's using permutations and SBOX:s (substitution tables). Feistel network appeared originally in DES block cipher, it was later reused in Blowfish cipher and later in **Kasumi**, which was recently a standard block cipher in 3G and 4G. Today Kasumi is replaced by AES and SNOW3G.

Feistel algorithm has 16 rounds. Each round uses different subkey K_i derived from the master key K .

Each round starts with initial permutation and ends with final permutation (called P-BOX:s).

Between permutations there are eight S BOXes, which obscure the connection between the key and the ciphertext implementing Shannon's confusion principle.

Many block ciphers, such as DES and Blowfish utilize structures known as *Feistel ciphers*.

AES encryption standard

In late 1990's NIST organized a competition to choose a new block cipher standard. There were 6 finalist, from which the Rijndael algorithm was chosen as the new standard in 2001.

The winner got a new name *Advanced Encryption Standard* AES.

Advantages of AES

- * It has lots of versions AES128, AES196, AES256, AES512. With flexible key lengths it answer the challenges of increasing computing power
- * The security is based on provable, transparent mathematics

It is generally thought that AES will be used as the standard block cipher for a long time in the foreseeable future.

AES128 uses a 128 bit key

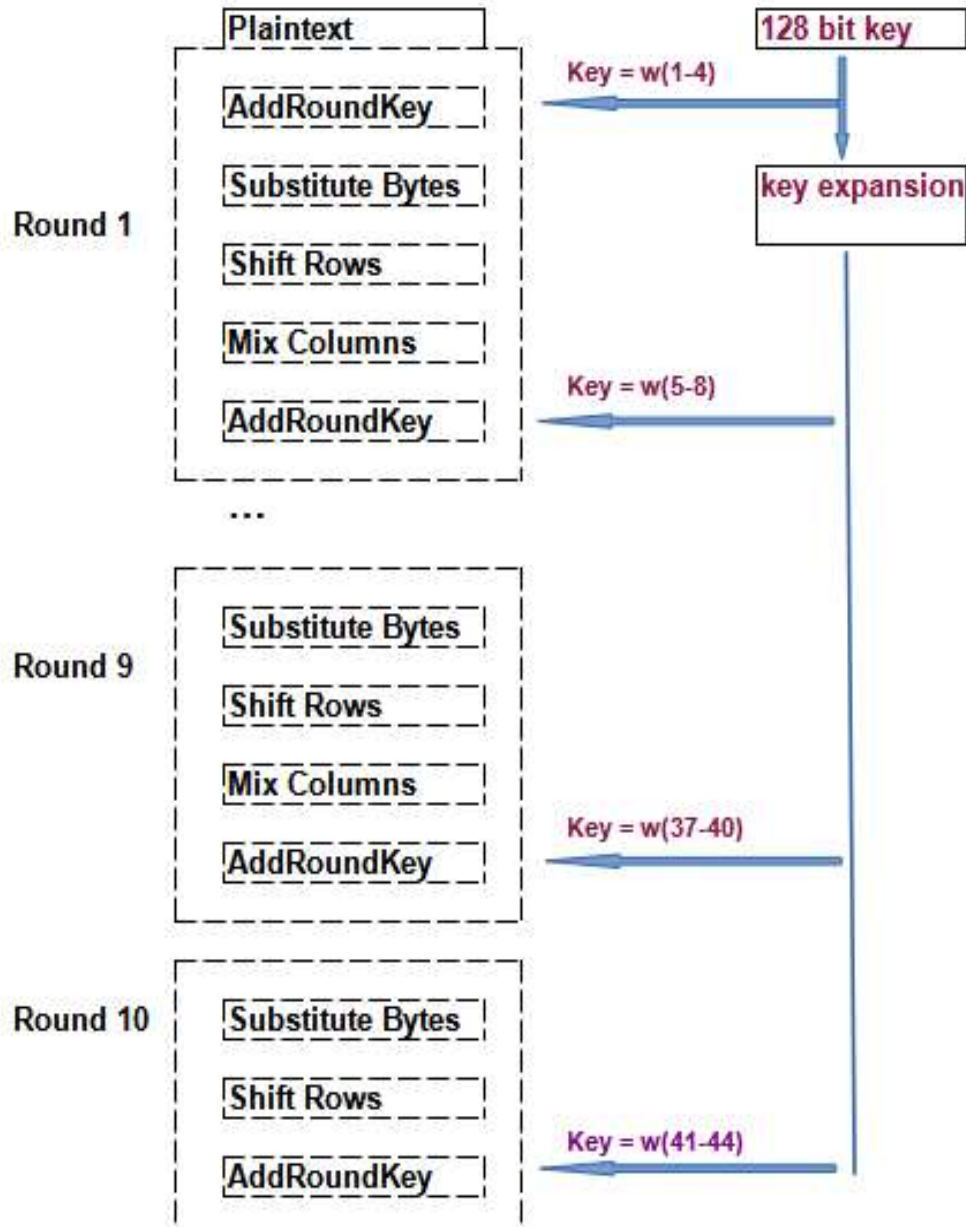
Algorithm has 10 rounds all of which use different subkeys derived from the primary key

Each round has many phases, which implement diffusion and confusion of bits

Phases of rounds are:

- Substitute bytes (Sbox)
- Shift rows
- Mix columns
- Add round key

The finest part, Sboxes uses Theory of Galois Fields. The algorithm in Sboxes was invented in 1991 by a Finnish cryptographer Kaisa Nyberg



Evariste Galois (1811-1832) was a great French mathematician who died at the age of 21

Round Key generation

AES128 algorithm has 10 rounds. Each round has an own round key, which is derived from the 128 bit master key K.

Round Key Generation is a quite complicated process, which can be described briefly as follows:

The 128 bit (=16 bytes) master key K is expanded to 44 words w_1, w_2, \dots, w_{44} . (1 word = 4 bytes = 32 bits) using a special algorithm. Details of the expansion can be found in internet, if you find this topic interesting.

Round1 uses 8 words of the expanded key: w_1, \dots, w_4 in the beginning and w_5, \dots, w_8 in the end of the round.

All the other rounds use four words each (see the picture in the previous slide)

Steps of AES rounds in pictures

ShiftRows step

Bytes in each row of the state are shifted cyclically to the left.

The amount of shift differs incrementally for each row.

No shift

Shift 1

Shift 2

Shift 3

| | | | |
|----------|----------|----------|----------|
| a_{11} | a_{12} | a_{13} | a_{14} |
| a_{21} | a_{22} | a_{23} | a_{24} |
| a_{31} | a_{32} | a_{33} | a_{34} |
| a_{41} | a_{42} | a_{43} | a_{44} |

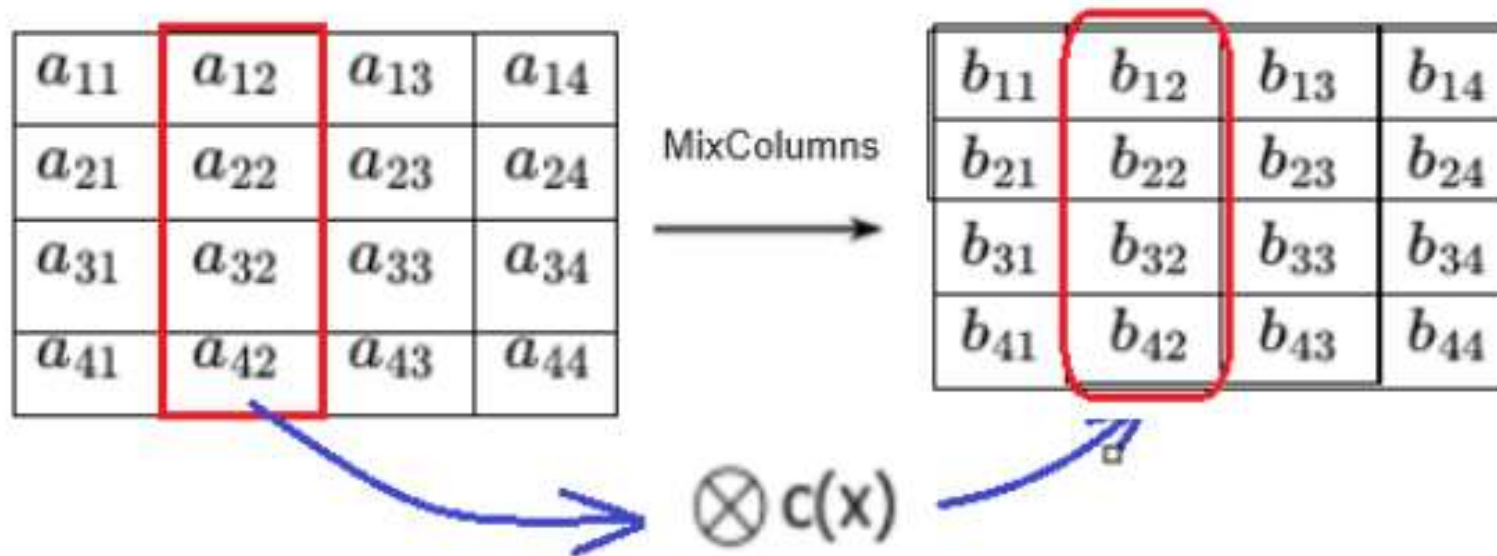
ShiftRows



| | | | |
|----------|----------|----------|----------|
| a_{11} | a_{12} | a_{13} | a_{14} |
| a_{22} | a_{23} | a_{24} | a_{21} |
| a_{33} | a_{34} | a_{31} | a_{32} |
| a_{44} | a_{41} | a_{42} | a_{43} |

MixColumns step

Each column of the state is multiplied with a fixed polynomial $c(x)$



Each column is presented as a polynomial. For example 2nd column of the state corresponds a polynomial $a(x) = a_{12}x^3 + a_{22}x^2 + a_{32}x + a_{42}$.

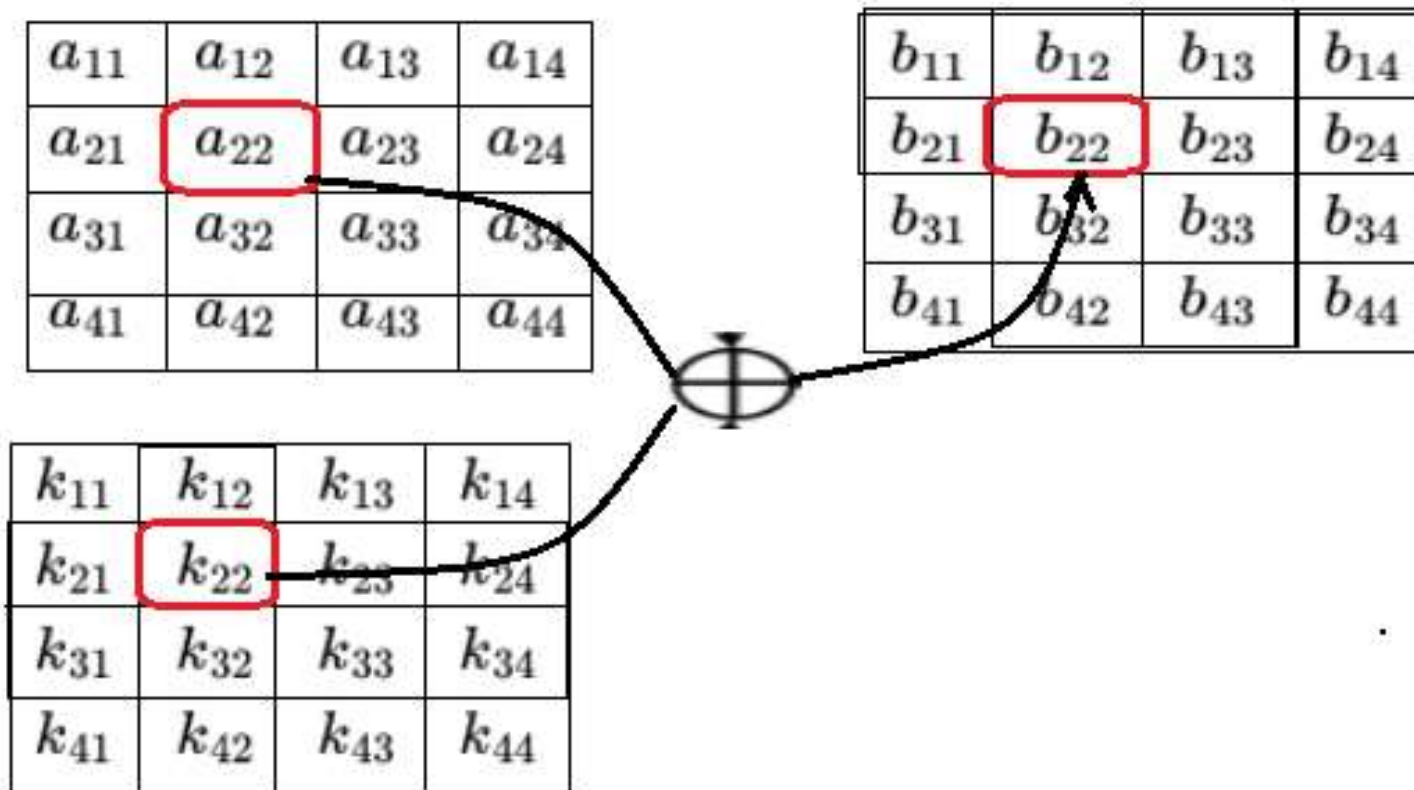
It is multiplied with a fixed polynomial $c(x) = 3x^3 + x^2 + x + 2$.

The product polynomial $a(x) \cdot c(x)$ is reduced by division with polynomial $x^4 + 1$.

The bytes $b_{12}, b_{22}, b_{32}, b_{42}$ of the resulting column consists of coefficients of polynomial remainder of the division.

AddRoundKey Step

Every round of AES has an own Round Key derived from the primary key. In AddRoundKey Step each byte of the state is combined with a byte of the Round Key using XOR – addition (symbol \oplus)



Mathematically most interesting is the Substitute Bytes step, which uses Galois field theory. (Finnish cryptographer Kaisa Nyberg has contributed to this step)

Multiplication rule of $a*b$ in field $GF(2^8)$ where a and b are 8 bit binary numbers.

Example: $a=11010100$, $b = 01101001$ (in integer form $a = 212$ and $b = 105$)

Step 1) a and b are interpreted as polynomials of 7th degree with binary coefficients.

$$a = x^7 + x^6 + x^4 + x^2, \quad b = x^6 + x^5 + x^3 + 1$$

Step 2) Normal polynomial multiplication is performed

$$(x^7 + x^6 + x^4 + x^2)(x^6 + x^5 + x^3 + 1) = x^{13} + 2x^{12} + x^{11} + 2x^{10} + 2x^9 + x^8 + 3x^7 + x^6 + x^5 + x^4 + x^2$$

Coefficients are converted to binary coefficients: even $\rightarrow 0$, odd $\rightarrow 1$. Thus

$$a*b = x^{13} + x^{11} + x^8 + x^7 + x^6 + x^5 + x^4 + x^2$$

Step2 A single WolframAlpha. command : `expand (x7 +x6 +x4 +x2)(x6 +x5 +x3 +1) mod 2` gives $x^{13} + x^{11} + x^8 + x^7 + x^6 + x^5 + x^4 + x^2$

Step3) The result of step2 is divided with a specific 8. degree polynomial called "Field Irreducible polynomial" which in AES is $x^8 + x^4 + x^3 + x + 1$

The remainder of division is the polynomial $x^6 + x^5 + x^4 + x^3 + x$ corresponding sequence 01111010 which is the product of a and b .

Step3 with W.A. Calculate the remainder using command

`remainder ($x^{13} + x^{11} + x^8 + x^7 + x^6 + x^5 + x^4 + x^2$)/($x^8 + x^4 + x^3 + x + 1$), which gives`

`$-x^6 + x^5 + x^4 - x^3 + 2x^3 + x$` Replacing even $\rightarrow 0$ and odd $\rightarrow 1$, we get a binary polynomial $x^6 + x^5 + x^4 + x^3 + x$, which corresponds 01111010.

Using integer forms for a , b and $a*b$ we can write $212*105 = 122$

Modes of operation

1) ECB : (Electronic Codebook mode)

Message blocks are encrypted independently => Identical message blocks have identical cipher blocks. This is why ECB mode is not secure and not used in block ciphers

2) CBC : Cipher Block Chaining mode (used in TLS until 2017)

Each cipher block functions as extra input of encryption of next block. The ciphers of first block affects all remaining blocks. This increases security.

The following line from 2017 describing algorithms of Nordea Bank's TLS connections

Tekniset tiedot

Yhteys salattu (TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, 256-bittinen avain, TLS 1.2)

3) GCM : Galois Counter Mode (today's standard in TLS)

In 2023 Nordea Bank's TLS uses AES in GCM mode

Tekniset tiedot

Yhteys salattu (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256-bittinen avain, TLS 1.2)

About AES_CBC and AES_GCM modes

One can still find TLS servers using AES_CBC .

Tekniset tiedot

Yhteys salattu (TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, 256-bittinen avain, TLS 1.2)

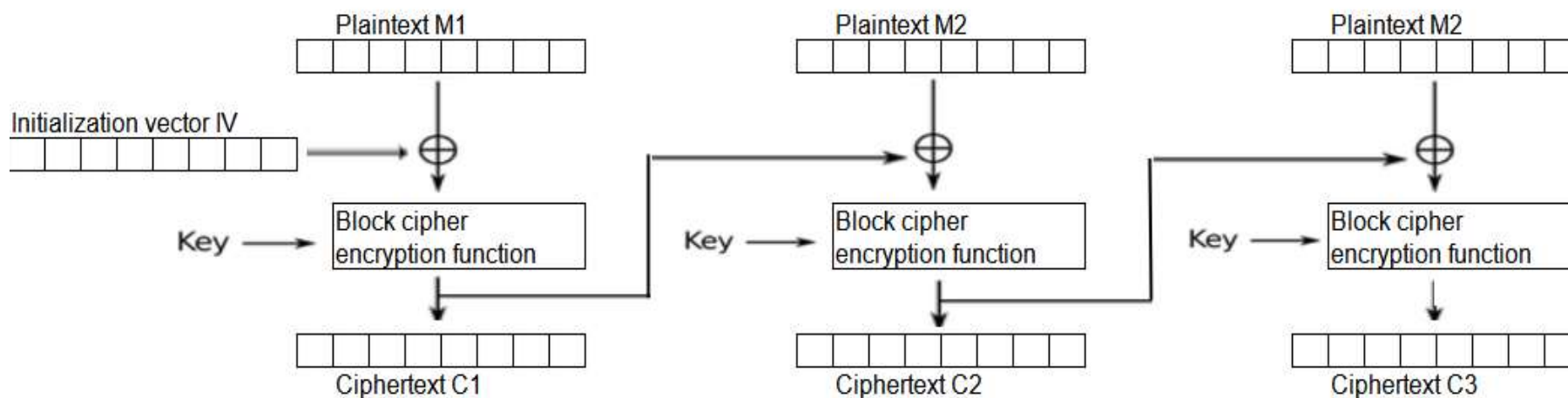


Diagram of CBC mode

Data is encrypted in 128 bit blocks. Input of each encryption are message, key, and the cipherblock of previous encryption (or IV). Every cipherblocks affects all next cipher blocks, which makes the encryption stronger against attacks and makes manipulations of some part of the cipher during transmission impossible..

GCM – mode ("Galois Counter Mode")

has replaced CBC mode in net banks providing stronger protection of integrity and authentication of sender.

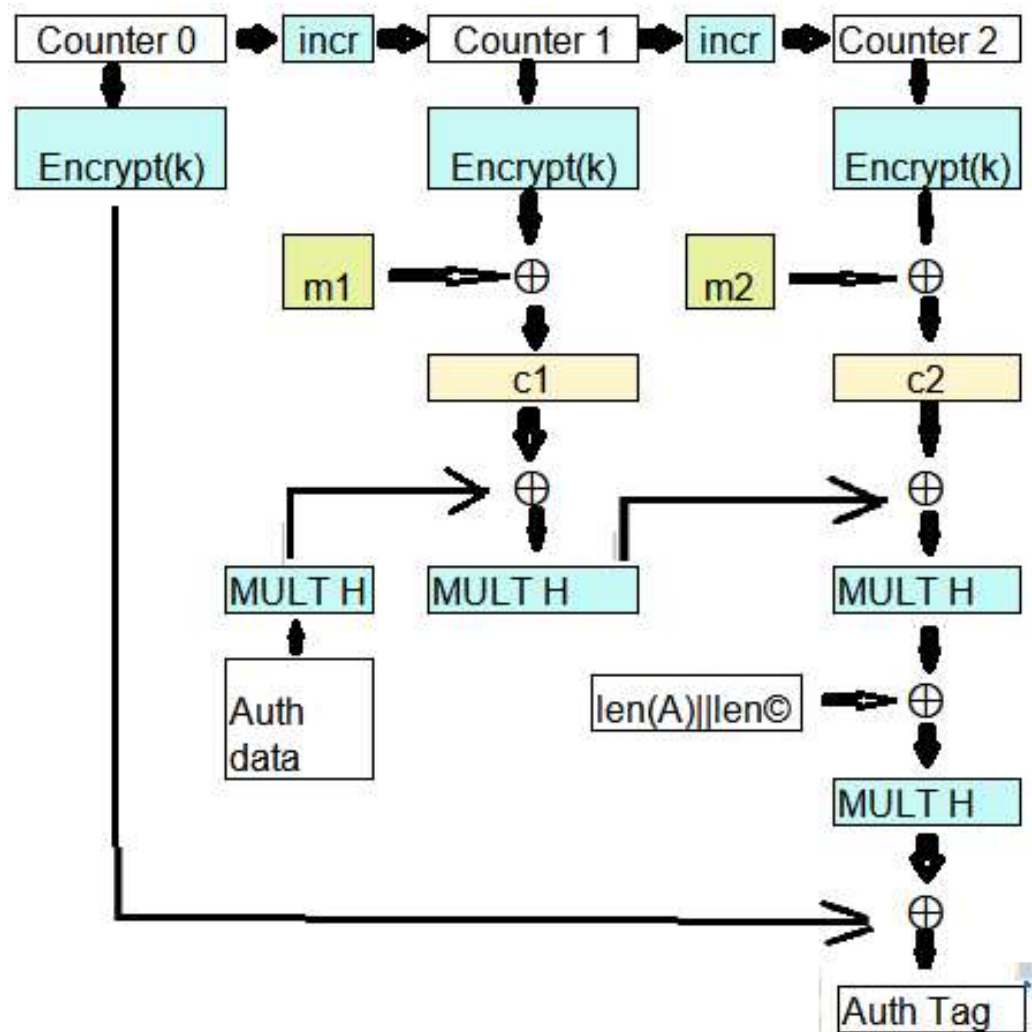
Tekniset tiedot

Yhteys salattu (TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, 256-bittinen avain, TLS 1.2)

In GCM- mode the counter value (1,2,...) is encrypted with AES with key K. The output (128 bits) is XOR:ed with the first message block m1 to produce the first cipher block c1.

Authentication data (senders personal data + previous cipher blocks) is collected to a 384 bit hash value using Galois Field multiplication rule.

The goals of this mode are to make attacks impossible and secure the integrity and authenticity of the sender



Finnish governments instructions for block ciphers

| National security classification | IV | III | II | I |
|-------------------------------------|-------------------------|-------------------------|-------------------------|---------|
| Block ciphers allowed | AES 128 Serpent(128) | AES 196 Serpent(196) | AES 256 Serpent(256) | none *) |

*) Top secret documents (class 1) should be kept only in paper form.

In practice the government uses AES encryption

Source: Cyper security center of Finland

Is AES post-quantum secure?

Quantum computers will be "game changers" in cryptography.

According to today's knowledge AES128 will no longer be secure in post-quantum world, but AES256 and AES512 still provide adequate security. *)

*) There is a quantum algorithm called Grover's algorithm, which can crack AES128 key in a short time using 128 qubit quantum computers (such computers don't exist yet)

However Grover's algorithm is not able to crack the AES256 key of 256 bit length. The security of AES256 remains at the level that corresponds AES128 in the present pre-quantum world.

Next topics:

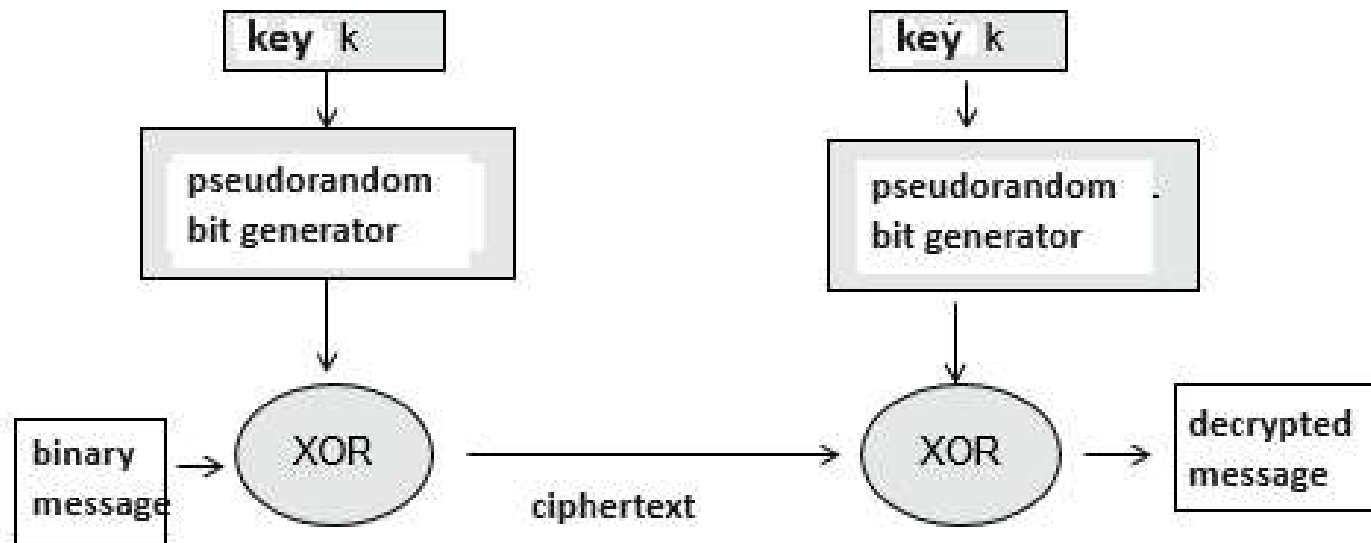
Synchronous stream ciphers

Pseudorandom number generation

LFSR registers

Mobile network encryption

Synchronous stream ciphers



The **encryption algorithm A5** of GSM phones is a synchronous stream cipher. It imitates the idea of Vernam's version of One Time Pad, in which key is an one time random bit sequence of same length as the message.

GSM phones have a micro circuit which produces a pseudorandom bit sequence, which is added with XOR to the binary message.

GSM call would be safer, if the key sequence would be truly random, which it is not.: Key sequence created by GSM phone looks random, but it is deterministic.

GSM calls are not secure, encryption of GSM calls can be broken. GSM network has been replaced by 3G, 4G and 5G networks, which are more secure.

Definition of pseudorandomness

PN- sequence (PN = "pseudo noise") or pseudorandom bit sequence is a key -based, deterministic bit sequence, which satisfies three properties defined by **Samuel W Colomb** in 1950's..

PN sequence properties:

G1. Sequence must have 50% ones 50% zeros

G2. Relative frequencies of blocks repeating same bit (0 or 1)

| | | | |
|--|----|--------|----------------------------|
| 010 | or | 101 | single bit block |
| 0110 | | 1001 | two identical bits block |
| 01110 | | 10001 | three identical bits block |
| 011110 | | 100001 | four identical bits block |
| have ratios $1/2$, $1/4$, $1/8$, $1/16$ | | | |

G3. When a sequence is rotated and the rotated sequence is compared with the original, the number of incidences and disincidences should be approximately equal. This property is measured by so called autocorrelation coefficient, which should be close to zero for all rotations of sequence, which means that the sequence does not have internal periodicity.

Additional features required from cryptographic random number generators

4. All PRNG generators have a period. (They start to produce same numbers when period is full).

Period should be as large as possible

5. Random number generation should be **very fast**

6. It should be impossible to calculate next or previous random numbers knowing one of the numbers.

"Cryptographically secure random number generation"

Secure communication needs "**cryptographically secure**" **pseudorandom number generators (CSPRNG)** for example in creating symmetric keys for AES.
(Most pseudorandom number generators are not cryptographically secure).

Some CSPRNG methods

1. Entropy source method. Unpredictable data stream is collected mainly from computers operating system (key inputs, time stamps, interruptions, sensors,). This data is hashed to create random numbers.

2. "Stretching entropy". Data obtained from 1st method is limited, if lots of random numbers are needed at once. One can extend the quantity of random numbers using for example AES in counter mode. Each output is a random number..

Random key generation is critical issue for safe communication. A non-safe random number generator has been deliberately used for eavesdropping communication.

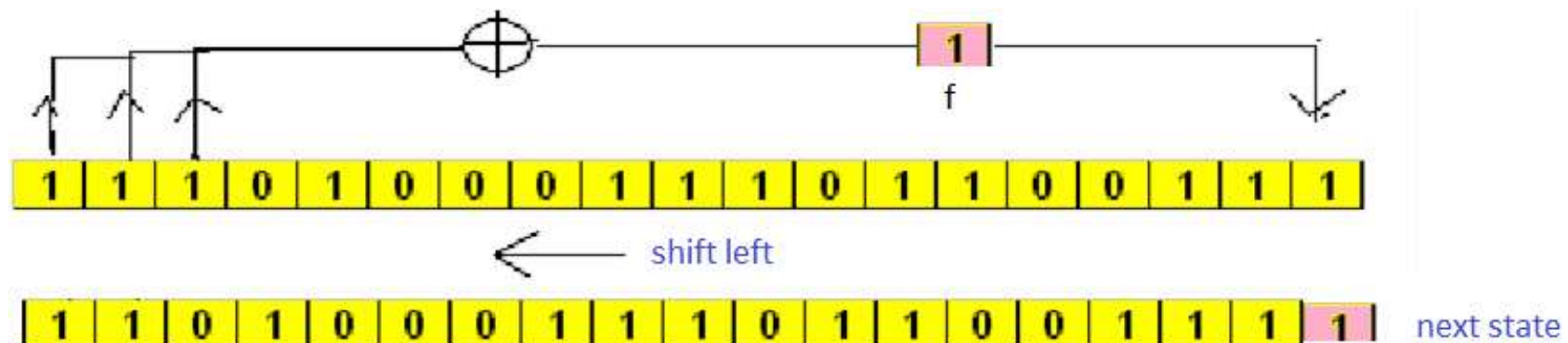
"The Guardian and The New York Times have reported in 2013 that the National Security Agency (NSA) inserted a backdoor into a pseudorandom number generator (PRNG) of NIST SP 800-90A which allows the NSA to readily decrypt material that was encrypted with the aid of Dual EC DRBG. Both papers report[30][31] that, as independent security experts long suspected,[32] the NSA has been introducing weaknesses into CSPRNG standard 800-90; this being confirmed for the first time by one of the top secret documents leaked to the Guardian by Edward Snowden." (Wikipedia)

LFSR - linear feedback shift register

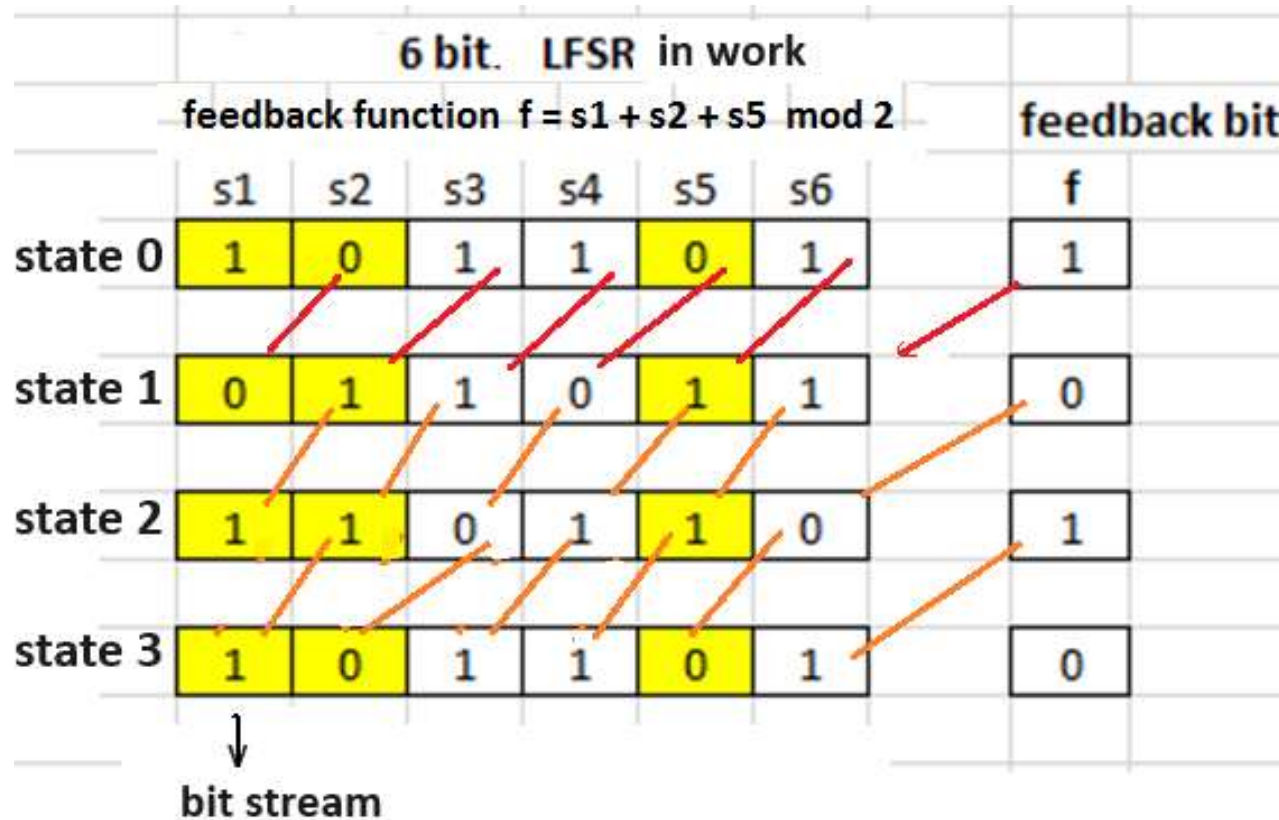
Is a microcircuit traditionally used in RAND function of pocket calculators and later in GSM phones

* LFSR is n bit register which can be used to produce random numbers. During every clock pulse the bits of the registers are shifted one step to the left. The new rightmost bit, called the feedback bit, is calculated using XOR addition from specific bit values just before the shift

In the picture feedback bit is calculated from first three bits. In the example feedback bit $f = 1 + 1 + 1 \bmod 2$ which is equal to 1.



Example of LFSR in operation



Feedback bit is calculated using formula

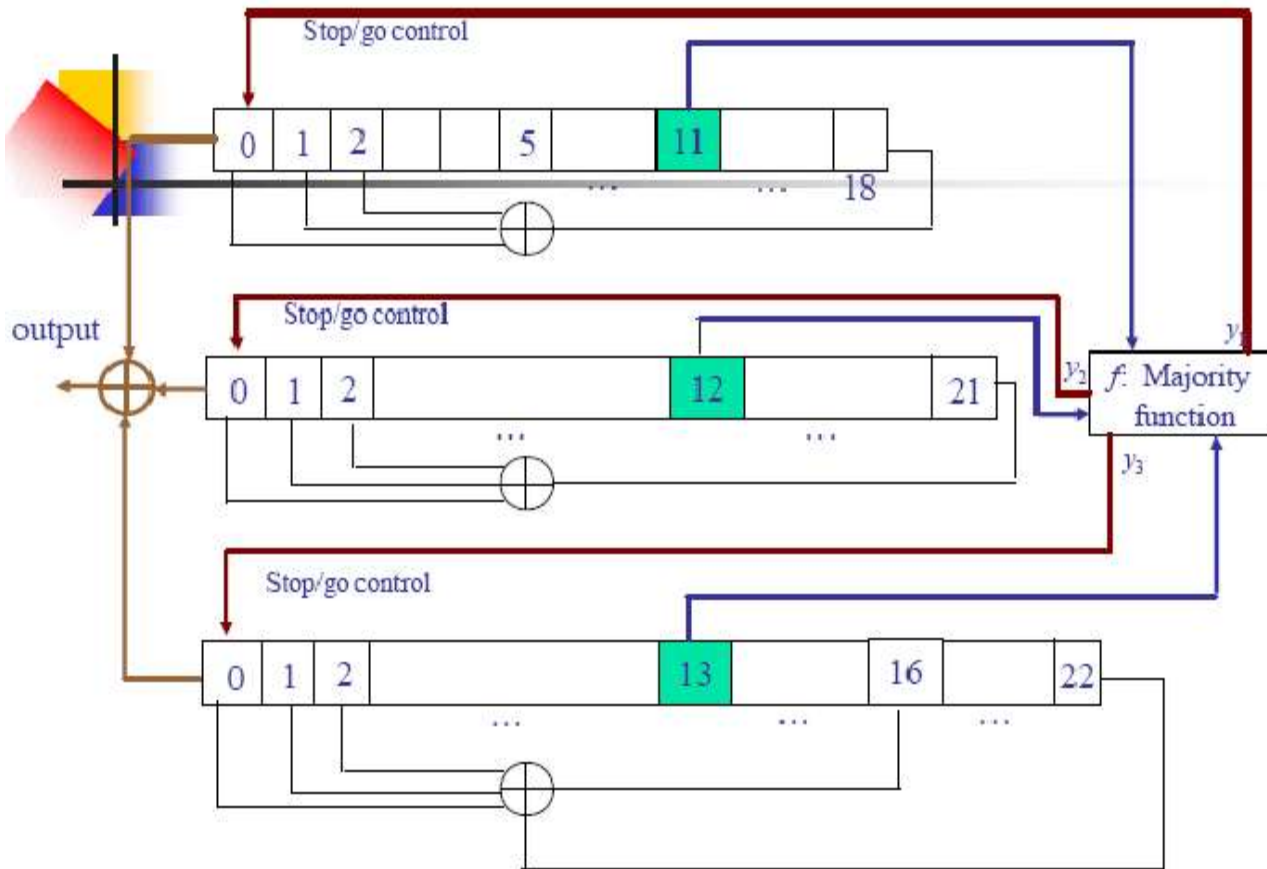
$$f = s_1 + s_2 + s_5 \pmod 2$$

before bits are shifted to left.

LFSR registers leftmost s1 bits form a sequence, which fulfills the three properties of definition of pseudorandomness.

LFSR registers were used earlier in GSM phones. Today some 3G, 4G and 5G networks use SNOW3G encryption, which also uses LFSR registers.

GSM phones A5 PRNG-generator



**GSM – phone has 3 LFSR-
registers** of lengths 19, 22 and
23 bits

**Initial state is the 64 bit
symmetric key.** $19 + 22 + 23 = 64$

**At each clock pulse circuit
generates one pseudo random
bit, which is a XOR-sum of zero
bits.**

**To increase security a majority
function f is added to the circuit.**
It is calculated from bits marked
green in the picture, which of the
three registers are shifted during
one clock pulse and which remain
as they are.

Majority function: If all marked green bits have identical values, all registers move forwards. In other cases those two move, which have identical values .

A5 bit stream fulfills pseudorandomness postulates G1, G2, G3

0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1,
1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1,
1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0,
1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1,
1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0,
1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1,
1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0,
0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1,
1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0,
1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1,
0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1,
1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0,
1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0,
1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1,
1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0,

GSM encryption: The key stream and digitalized voice are added using XOR to produce the encrypted signal

Operators server has a similar PRNG and same symmetric initial state
Operator decrypts signal using XOR.
Signal is encrypted only in air, not in the cable.

GSM security

1. Key in A5 encryption is 64 bits, which is not secure.
2. Key sequence is periodic, effective period is $4/3 \cdot 2^{23}$
3. GSM signal is encrypted only between the mast and the phone (not in cables)
4. GSM is not secure against professional hackers

Authentication and key agreement in GSM

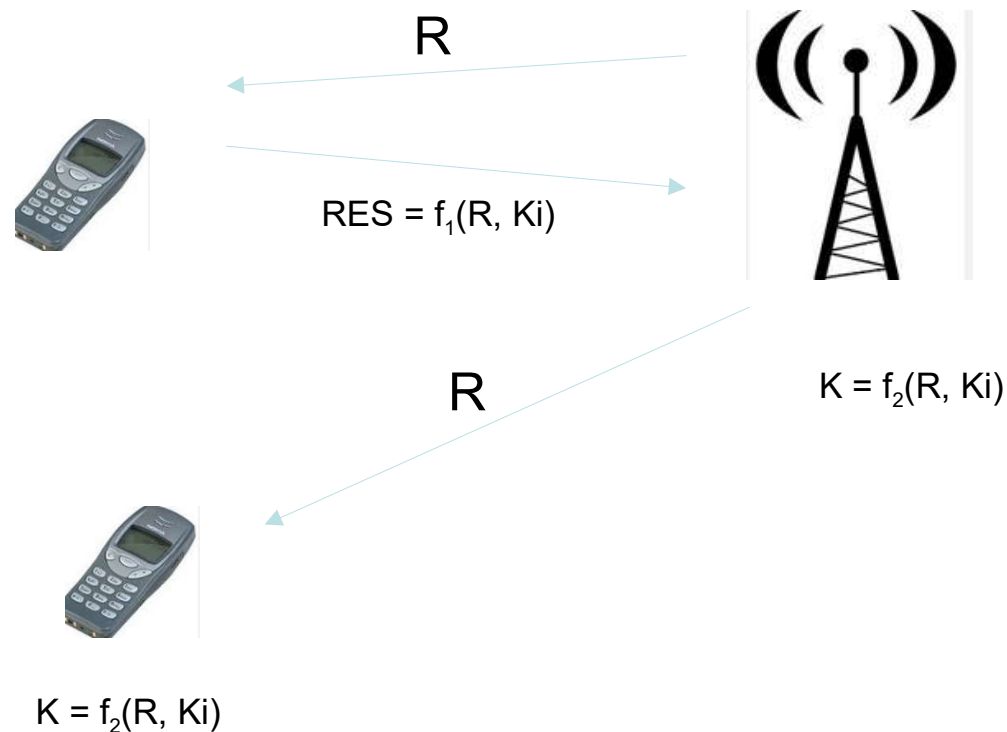
Authentication A3. Operator sends to the phone a random challenge number R.

Phone calculates and sends a response RES from R and SIM-key.

Operator calculates RES in the same way. If there is a match, the phone is authenticated.

Key agreement A8. Operator sends the phone a random R. The phone calculates a 64 bit key K from R and SIM-key.

The key K is the initial state for the three LFSR -registers



3G, 4G, 5G network encryption

3G and 4G use block ciphers: AES128 or SNOW3G

- key length = 128 bits
- two way authentication is used: both the phone and the mast authenticate themselves in the beginning of communication

5G encryption uses 256 bit versions of AES and SNOW3G

*SNOW3G is a Swedish encryption algorithm created in Lund university.
It uses LFSR register technology*