Fundamentals of Security in Communication Systems

overview tutorial
AUST

22.4. 2001
UAE

Wael Adi

Outlines

- **The Story of Security Science**
- **Traditional Secret Key Systems**
- **Public Key Systems**
- **Protocols**
  - Identification
  - Secrecy
- **Modern Standards**

Communication Security Objectives

- ***Secrecy***
- ***Authentication***

Employs Cryptographic mechanisms

IT Security Business

- **Increases very rapidly such as: *E-commerce, M-Commerce***
  => Security business in IT is increasing exponentially !

- **We still have serious security gaps :**
  - **e.g. Virus damage per year is 1.6 Billion $**
  - ***"I love you"* Virus damage was in year 2000 about 2 600 Mil. $**

Can We trust Modern Information Technology ?

Answer at the end of presentation

Cryptography : The Story of Security Science

- **Cryptography ?... A Science ?**

I. Conventional Cryptography as Art

- Julius Caesar Cipher
- Kaisiski " The *Art* of Deciphering" 1863, ... Gauss
- Vernam 1926, *first* and *last* unbreakable system
- II world ware 1945, Enigma, Hagelin .... Alan Turing

II. As a Science 1949

- **Revolution: Shannon (AT&T) 1948** 'A Mathematical Theory of Communication'
- **Shannon (AT&T) 1949** 'Communication Theory of Secrecy Systems´

III. Breakthrough to Modern Cryptology 1976

- Diffie and Hellmann 1976 "Public key Cryptography (Stanford University)"
- Revolution: ´Secured Communication without Prior Secret Agreement´

Cryptographic Security

Unconditionally secure:

System ***impossible*** to break with ***any*** means (whatever)

One impractical System is only known !

Practically Secure:

System ***possible*** to break with ***any*** means (whatever)

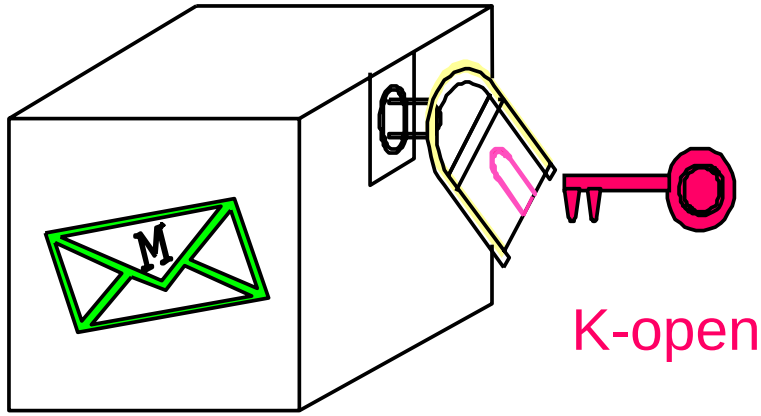
Many modern practical systems are known

Conventional Secret Key Cryptography

Fundamental Concepts

Secret Key Cryptography

(Symmetric System)



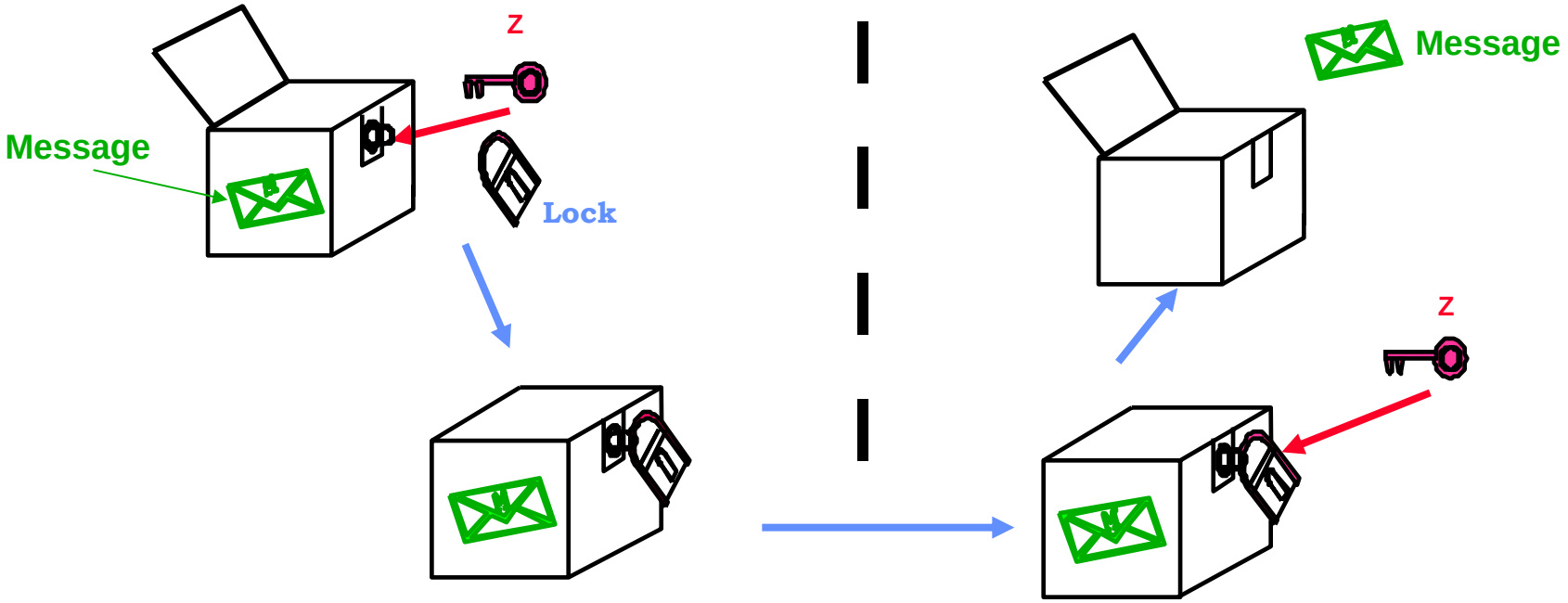
K-open = K-close

Open and close with the same key

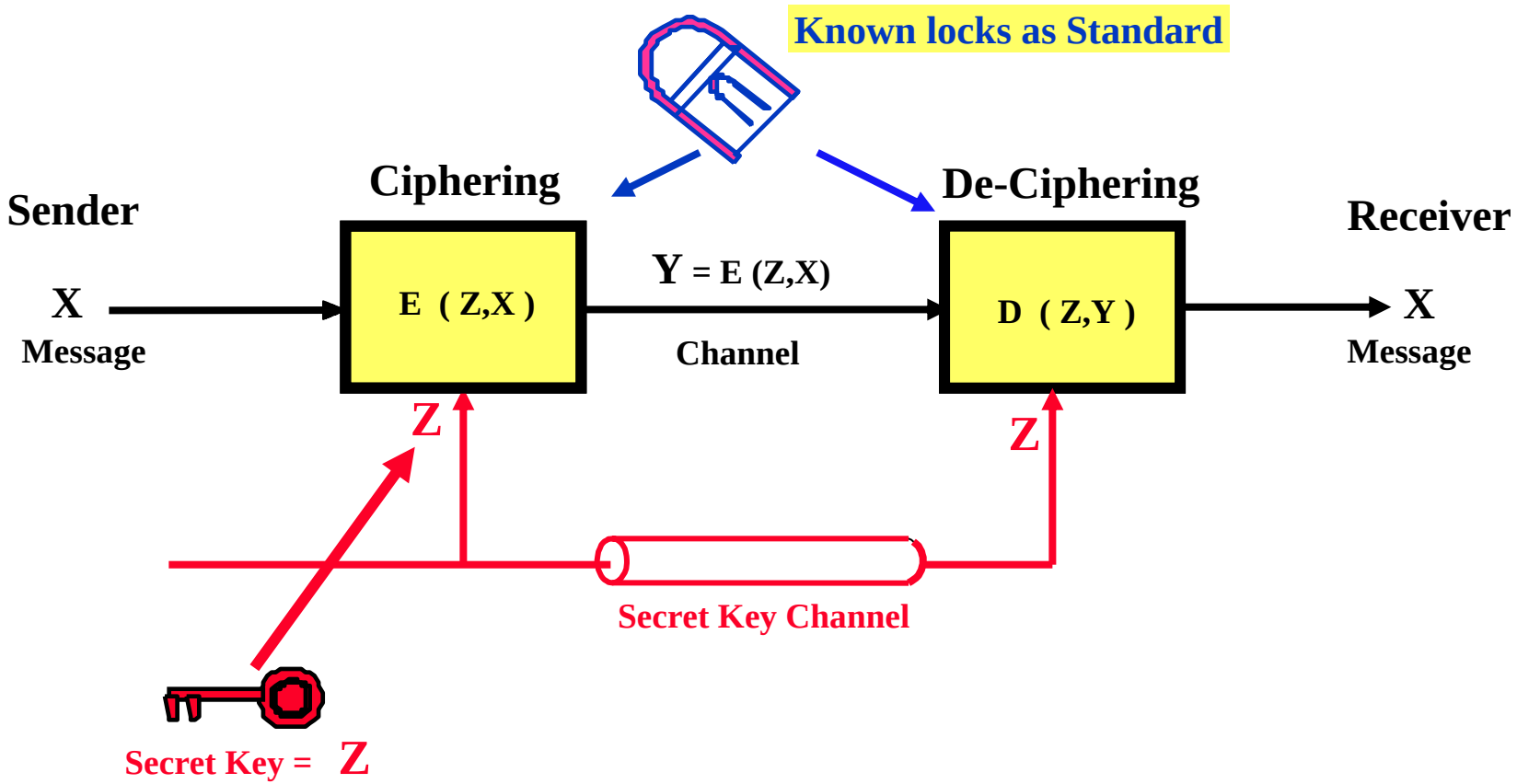
Secret Key Crypto-System : mechanical analog

SENDER ***RECEIVER***

Key = Z ⟷ Secret key agreement ⟷ Key = Z

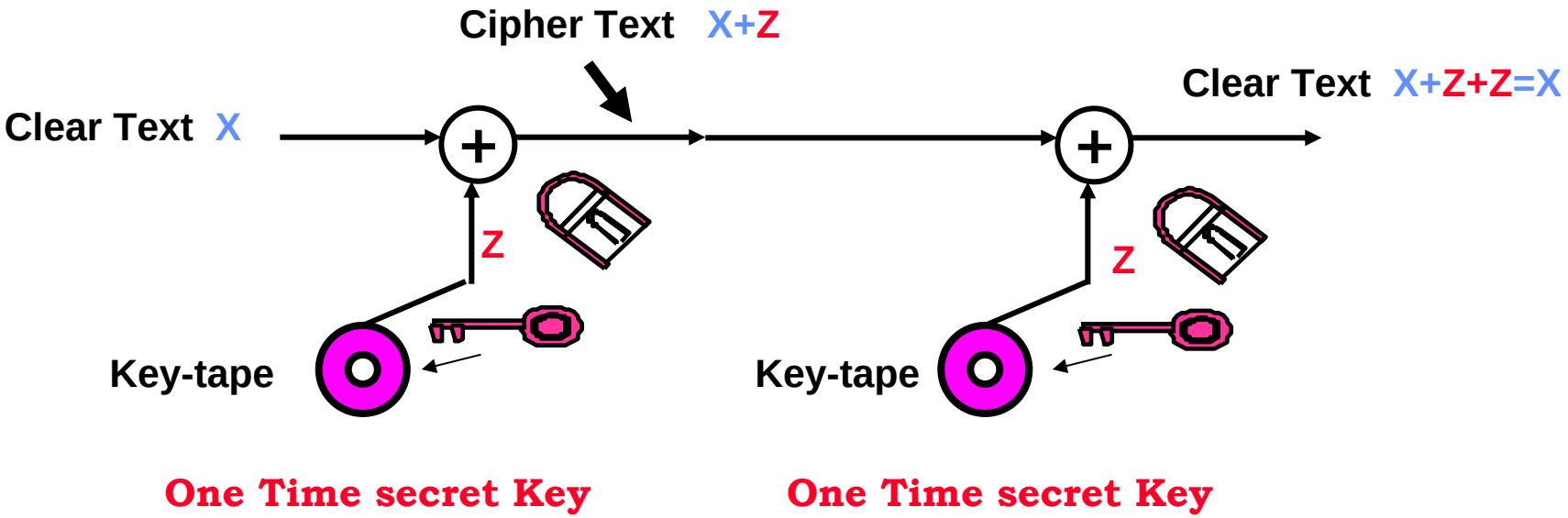


Conventional Cryptography till 1976 : Secret Key systems



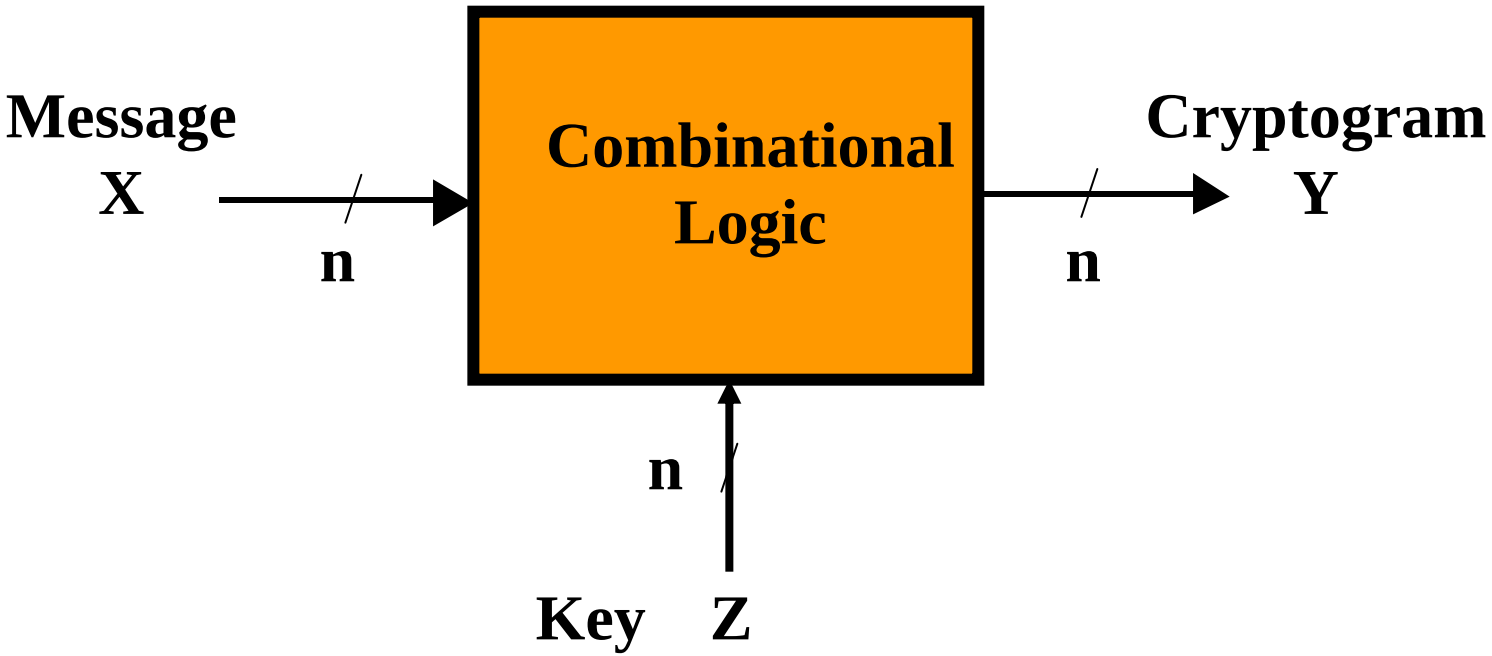
The Perfect Cipher: Vernam (AT&T 1926)

proved to be unbreakable by Shannon (AT&T 1949)



Key length = Clear text length (Shannon 1949)

Block-Ciphers



Standard Block-Ciphers

- **DES :** **D**ata **E**ncryption **S**tandard, IBM (NIST) 1976 (USA)
- **IDEA** (J. Massey and Lai) 1990 (Europe)
- **FEAL** NTT 1989 (Japan)
- **A5** GSM (Secret Cipher) (Europe)

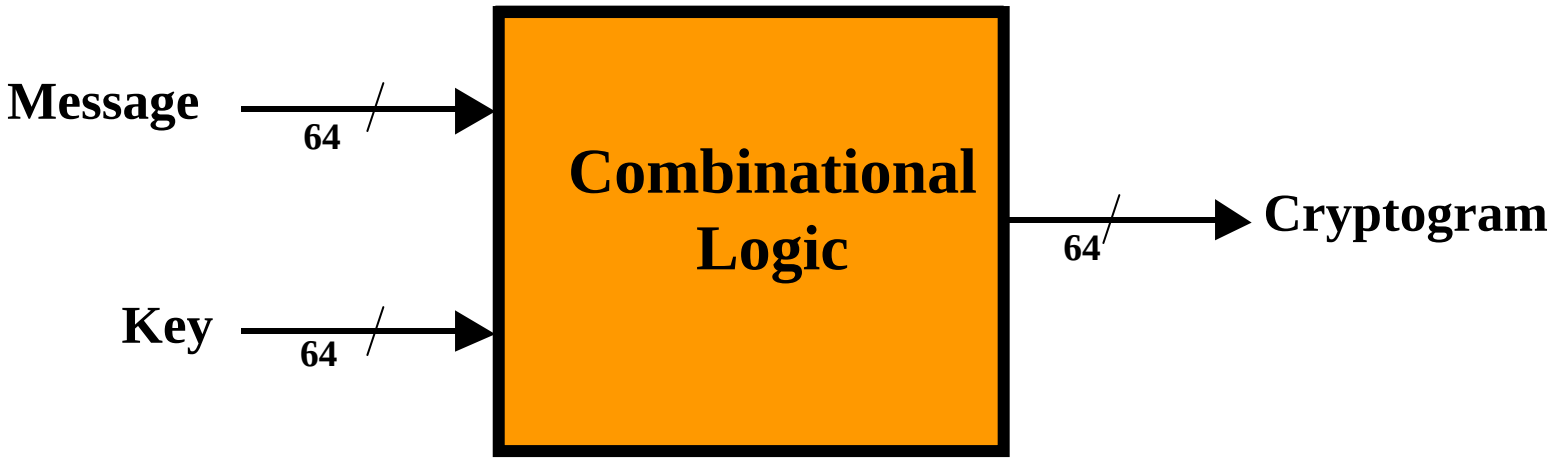
  Replaed by **KASUMI** 1999 UMTS/3GPP (Mitsubishi Japan)

- **AES** **A**dvanced **E**ncryption **S**tandard **(NIST):**

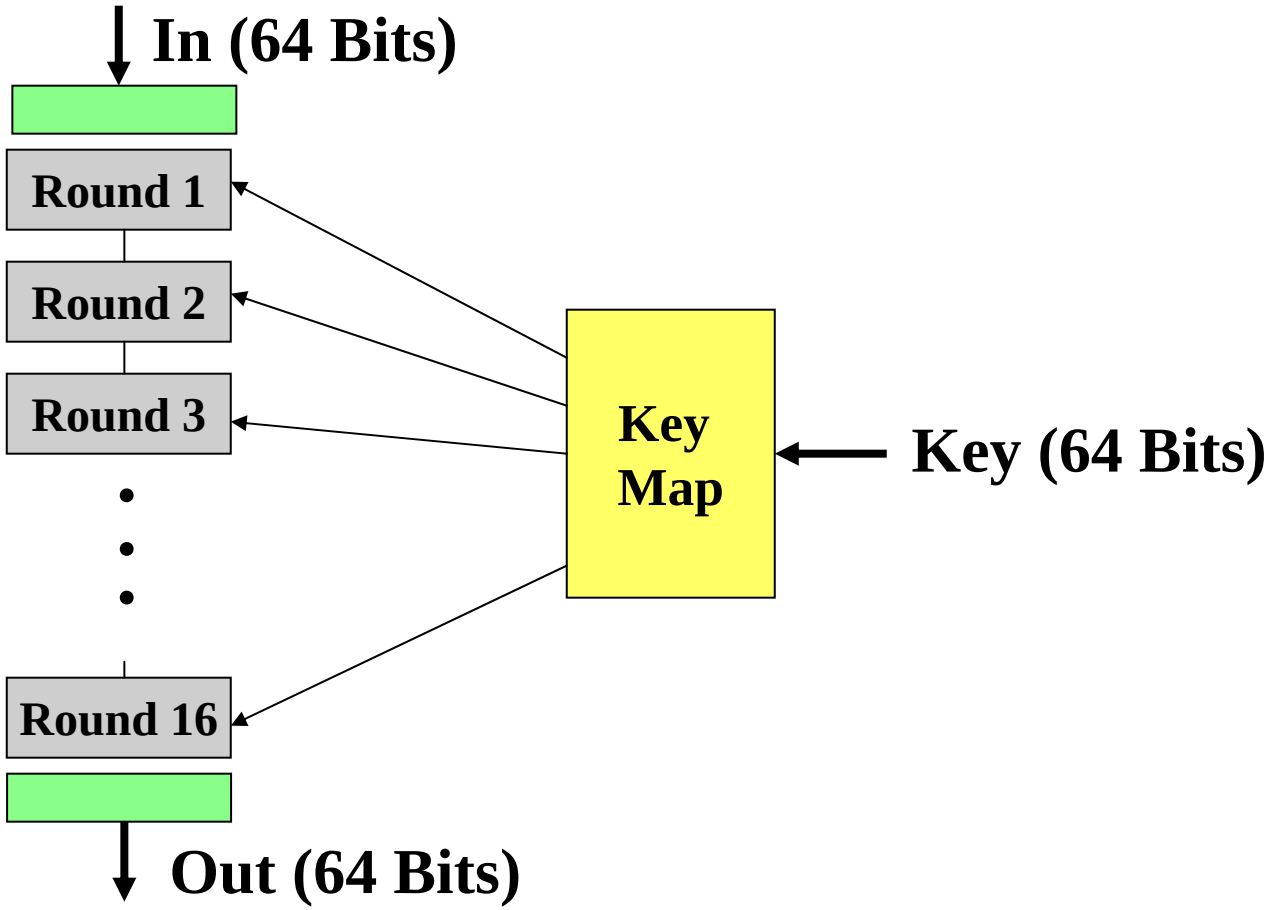
  New international standard **Rijndael** **Belgium (Oct. 2000)**

DES: Data Encryption Standard

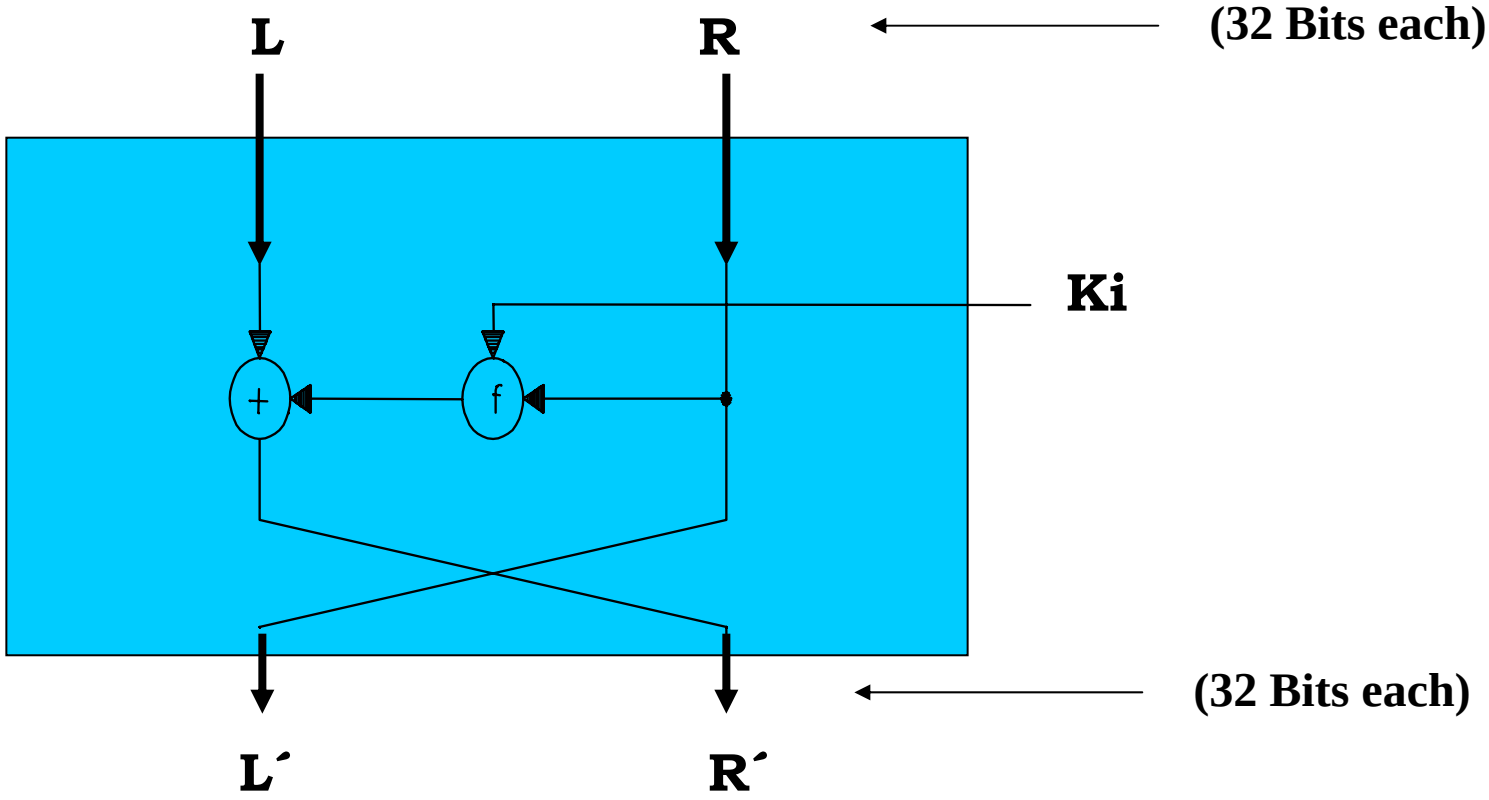
1976 NIST / IBM



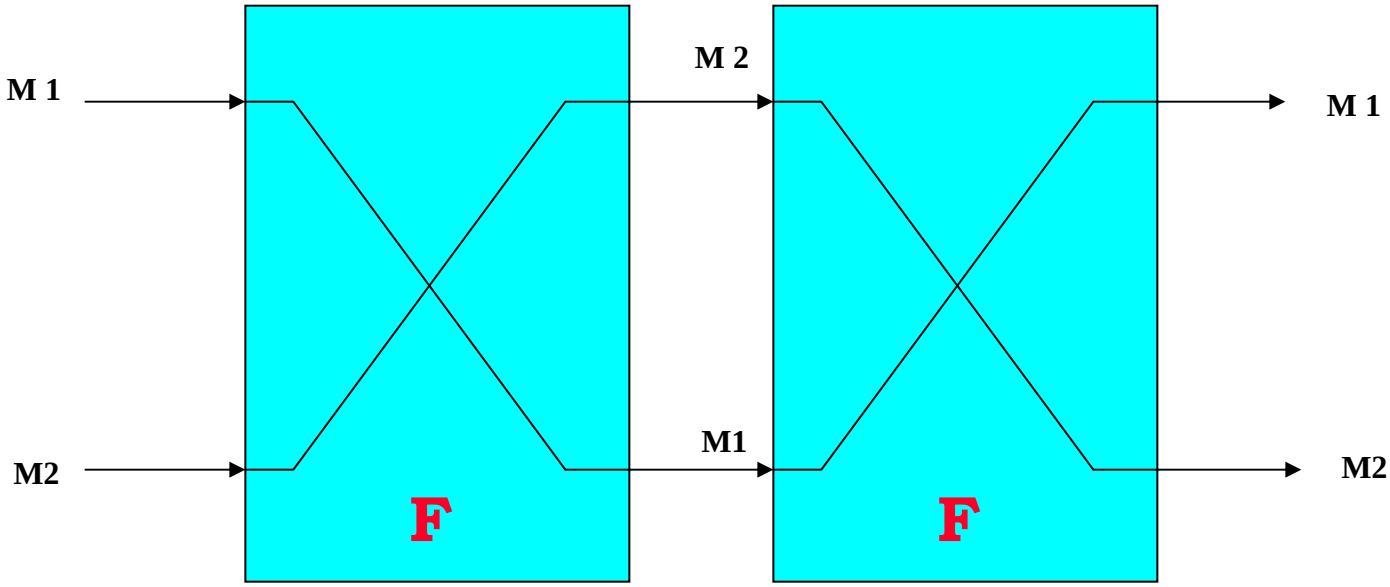
The Core of DES Cipher



DES Round Structure

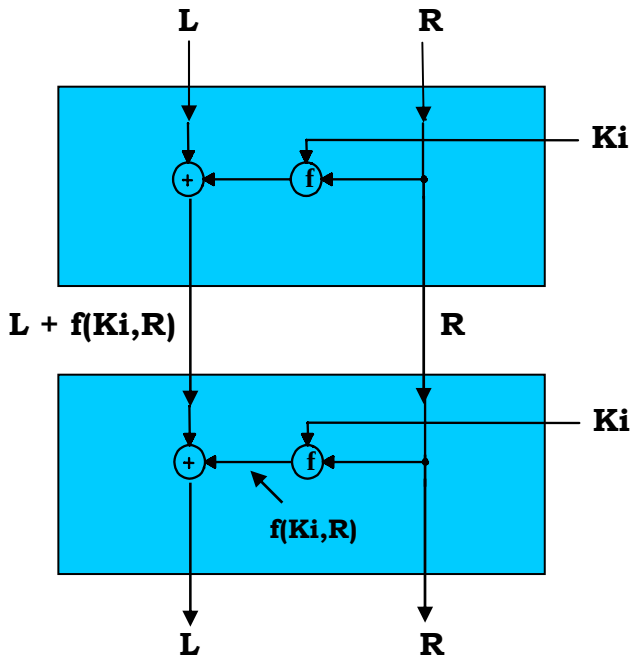


Involution



$$F \quad x \quad F \quad = \quad 1 \quad \Rightarrow \quad F = F^{-1}$$

Involution



DES is *still* not broken !!

and there is

No proof that DES can not be broken !!

This Dilemma characterises virtually all practical crypto-systems

GSM A5

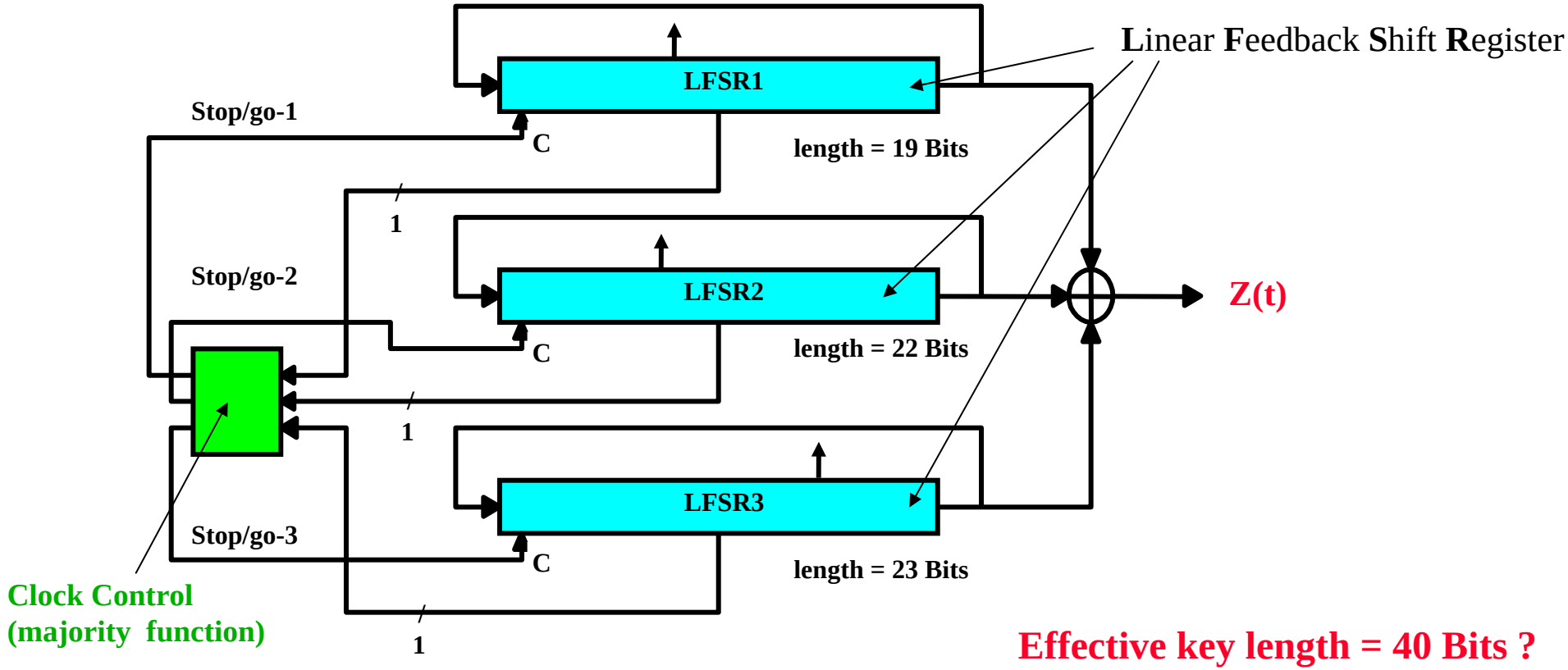
Mobile Confidentiality Cipher

A bad example of secret Cryptography:

!! A5 structure was never been made public !!

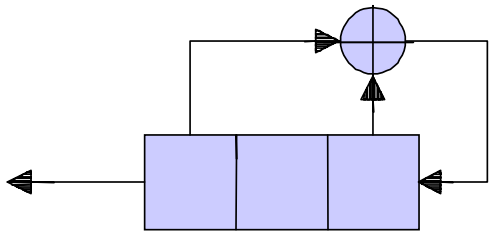
GSM: Mobile Phone A5 Stream-Cipher

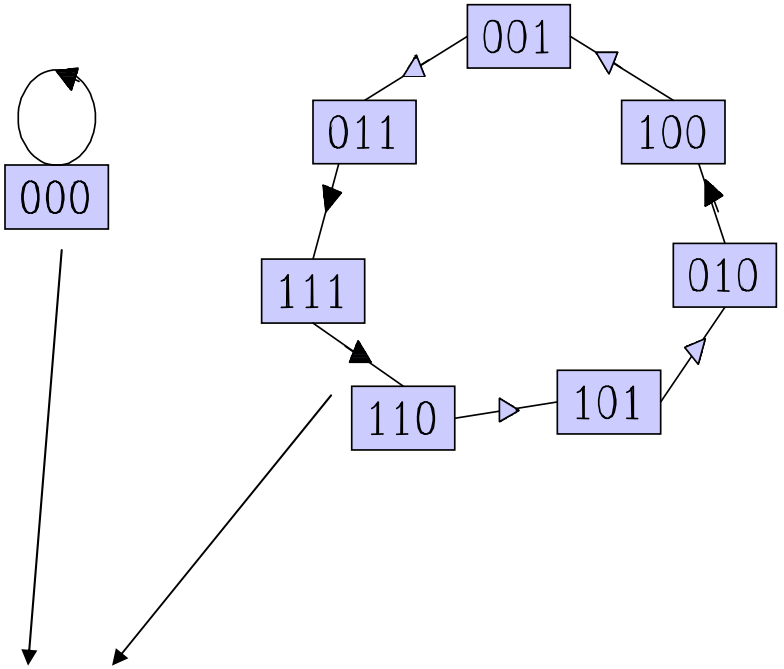
Published by Berkely Students, Attacked by Shamir 1999



Effective key length = 40 Bits ?

Basic Linear Feedback Shift Register LFSR Example





$C(D) = D^3 + D + 1$
is a primitive Polynomial with Period N
$= 2^3-1 = 7$.

Cycle structure is {1(1), 1(7)}.

KASUMI Cipher

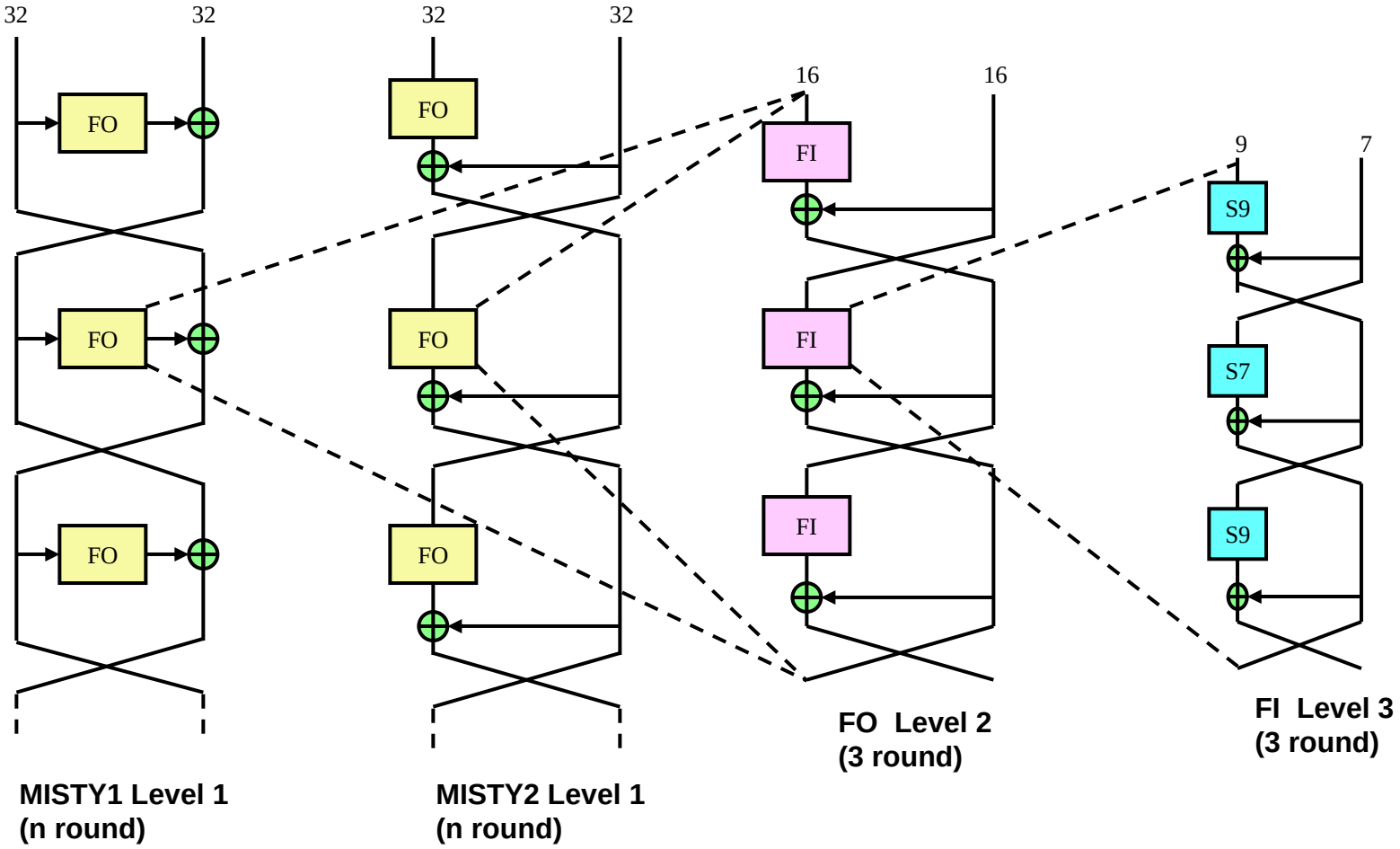
to replace A5

Original Cipher: Mitsubishi's " MISTY" 1997

Standardized for UMTS/3GPP (March 2000)

MISTY ⟷ KASUMI

Recursive Structure of MISTY



Structure of MISTY

Table of S7 over GF (2^7)

27, 50, 51, 90, 59, 16, 23, 84, 91, 26,114,115,107, 44,102, 73,
31, 36, 19,108, 55, 46, 63, 74, 93, 15, 64, 86, 37, 81, 28, 4,
11, 70, 32, 13,123, 53, 68, 66, 43, 30, 65, 20, 75,121, 21,111,
14, 85, 9, 54,116, 12,103, 83, 40, 10,126, 56, 2, 7, 96, 41,
25, 18,101, 47, 48, 57, 8,104, 95,120, 42, 76,100, 69,117, 61,
89, 72, 3, 87,124, 79, 98, 60, 29, 33, 94, 39,106,112, 77, 58,
1,109,110, 99, 24,119, 35, 5, 38,118, 0, 49, 45,122,127, 97,
80, 34, 17, 6, 71, 22, 82, 78,113, 62,105, 67, 52, 92, 88,125

Table of S9 over GF (2^9)

451,203,339,415,483,233,251, 53,385,185,279,491,307, 9, 45,211,
199,330, 55,126,235,356,403,472,163,286, 85, 44, 29,418,355,280,
331,338,466, 15, 43, 48,314,229,273,312,398, 99,227,200,500, 27,
1,157,248,416,365,499, 28,326,125,209,130,490,387,301,244,414,
467,221,482,296,480,236, 89,145, 17,303, 38,220,176,396,271,503,
231,364,182,249,216,337,257,332,259,184,340,299,430, 23,113, 12,
71, 88,127,420,308,297,132,349,413,434,419, 72,124, 81,458, 35,
317,423,357, 59, 66,218,402,206,193,107,159,497,300,388,250,406,
481,361,381, 49,384,266,148,474,390,318,284, 96,373,463,103,281,
101,104,153,336, 8, 7,380,183, 36, 25,222,295,219,228,425, 82,
265,144,412,449, 40,435,309,362,374,223,485,392,197,366,478,433,
195,479, 54,238,494,240,147, 73,154,438,105,129,293, 11, 94,180,
329,455,372, 62,315,439,142,454,174, 16,149,495, 78,242,509,133,
253,246,160,367,131,138,342,155,316,263,359,152,464,489, 3,510,
189,290,137,210,399, 18, 51,106,322,237,368,283,226,335,344,305,
327, 93,275,461,121,353,421,377,158,436,204, 34,306, 26,232, 4,
391,493,407, 57,447,471, 39,395,198,156,208,334,108, 52,498,110,
202, 37,186,401,254, 19,262, 47,429,370,475,192,267,470,245,492,
269,118,276,427,117,268,484,345, 84,287, 75,196,446,247, 41,164,
14,496,119, 77,378,134,139,179,369,191,270,260,151,347,352,360,
215,187,102,462,252,146,453,111, 22, 74,161,313,175,241,400, 10,
426,323,379, 86,397,358,212,507,333,404,410,135,504,291,167,440,
321, 60,505,320, 42,341,282,417,408,213,294,431, 97,302,343,476,
114,394,170,150,277,239, 69,123,141,325, 83, 95,376,178, 46, 32,
469, 63,457,487,428, 68, 56, 20,177,363,171,181, 90,386,456,468,
24,375,100,207,109,256,409,304,346, 5,288,443,445,224, 79,214,
319,452,298, 21, 6,255,411,166, 67,136, 80,351,488,289,115,382,
188,194,201,371,393,501,116,460,486,424,405, 31, 65, 13,442, 50,
61,465,128,168, 87,441,354,328,217,261, 98,122, 33,511,274,264,
448,169,285,432,422,205,243, 92,258, 91,473,324,502,173,165, 58,
459,310,383, 70,225, 30,477,230,311,506,389,140,143, 64,437,190,
120, 0,172,272,350,292, 2,444,162,234,112,508,278,348, 76,450

Expect
KAZUMI
in your 3rd Generation Mobile Phone
2003

KASUMI

is Publicly Evaluated

- Still not broken !!
- No proof that KASUMI can not be broken !!

Two contradictory statements !!

Hold virtually for all practical security systems

Advanced Encryption Standard

National Institute of Science and Technology NIST

1998-2001

AES Winner Algorithm:
The Rijndael Block Cipher
Decision Oct. 2000

AES Round-3 Finalist Algorithms (finalized in 2001)

- Symmetric-key ciphers 128, 192, and 256 bit keys
- Royalty-Free (i.e. public domain)

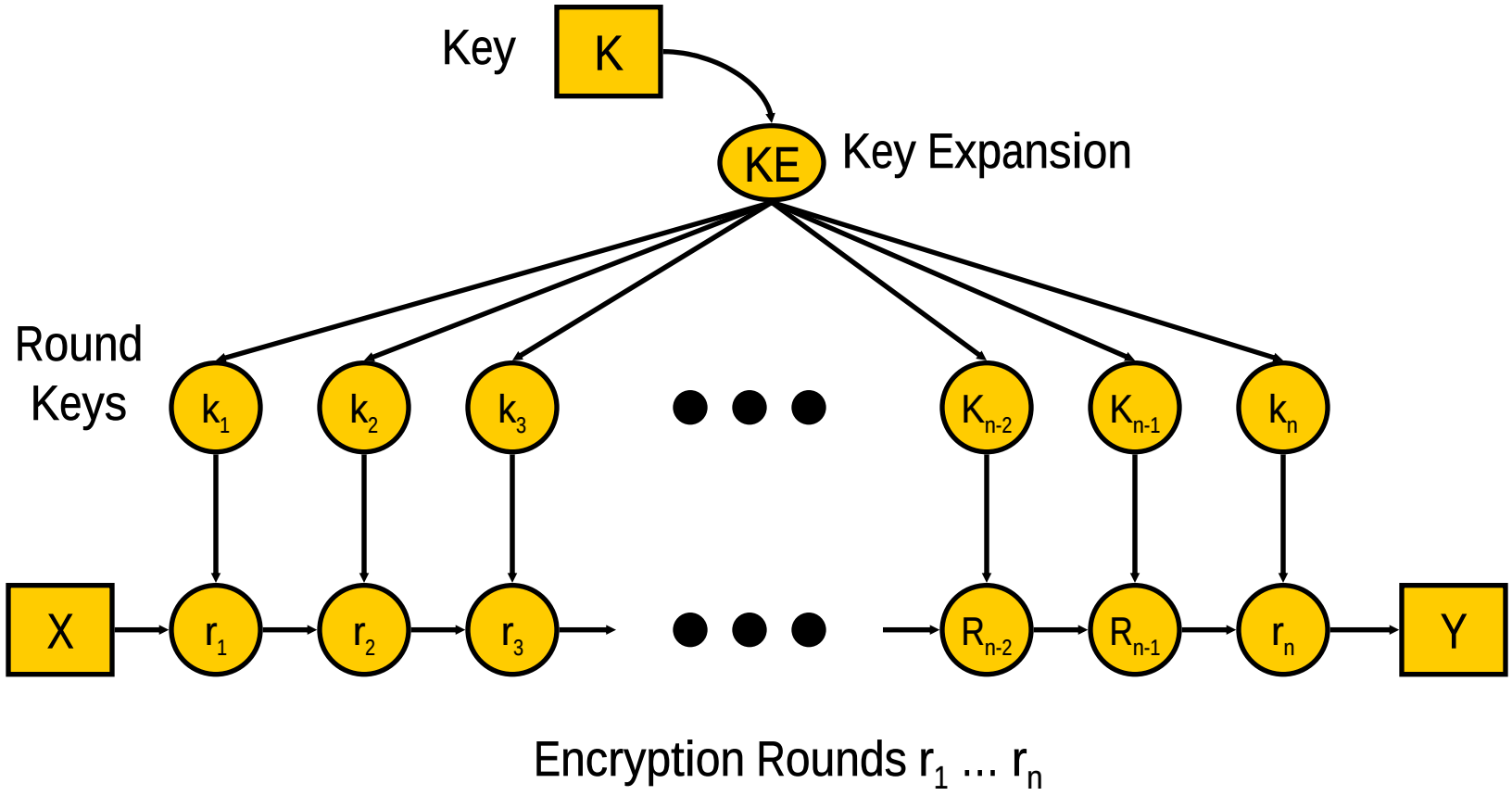
– MARS : IBM (USA)
– RC6 : R. Rivest (MIT), creator of the widely used RC4 (USA)
– Twofish : Counterpane Internet Security, Inc. (USA)
– Serpent : Ross Anderson, Eli Biham and Lars Knudsen (USA)

– Rijndael: Designed by J. Daemen and V. Rijmen (Belgium)

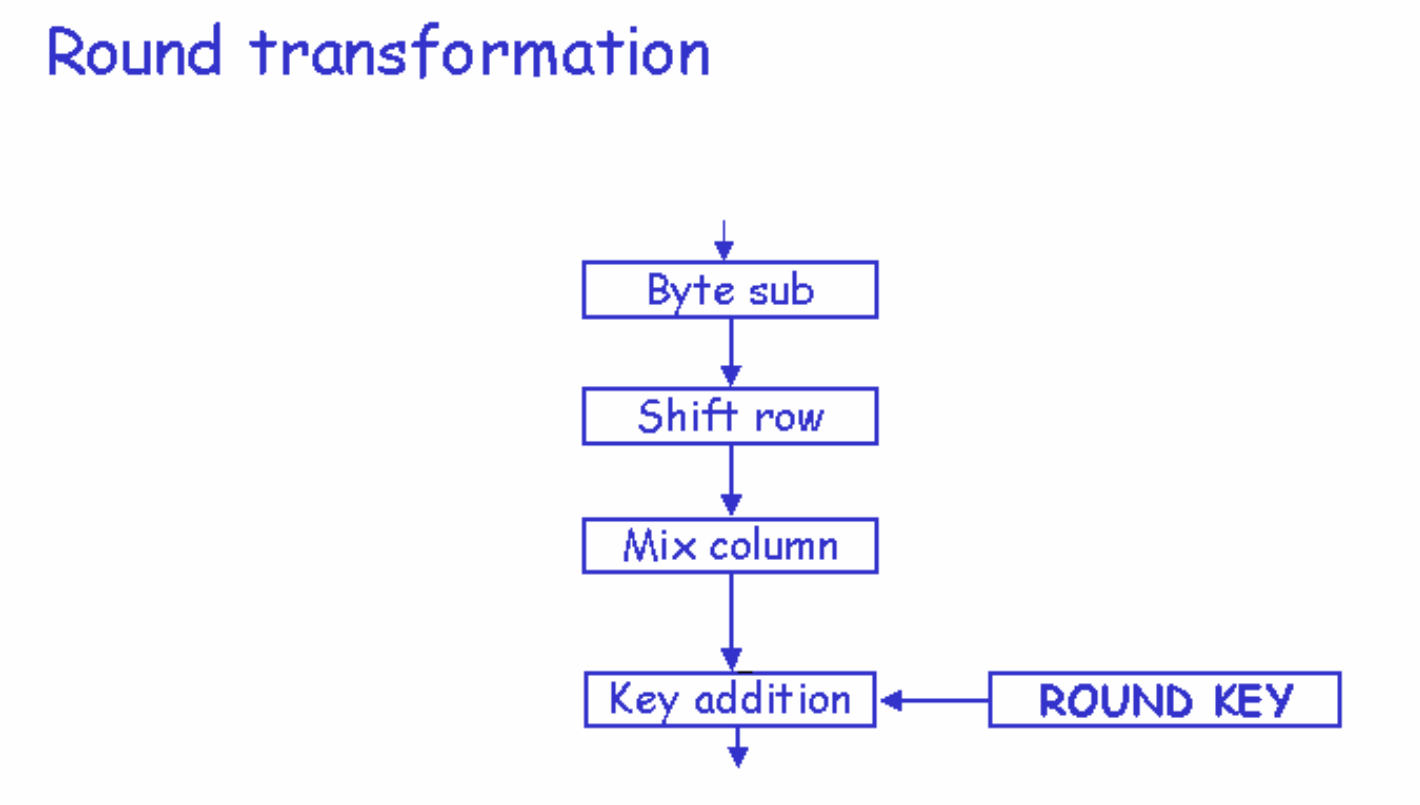
The Winner: Rijndael

- J. Daemen (Proton World International)
  & V. Rijmen (Katholieke Universiteit Leuven).

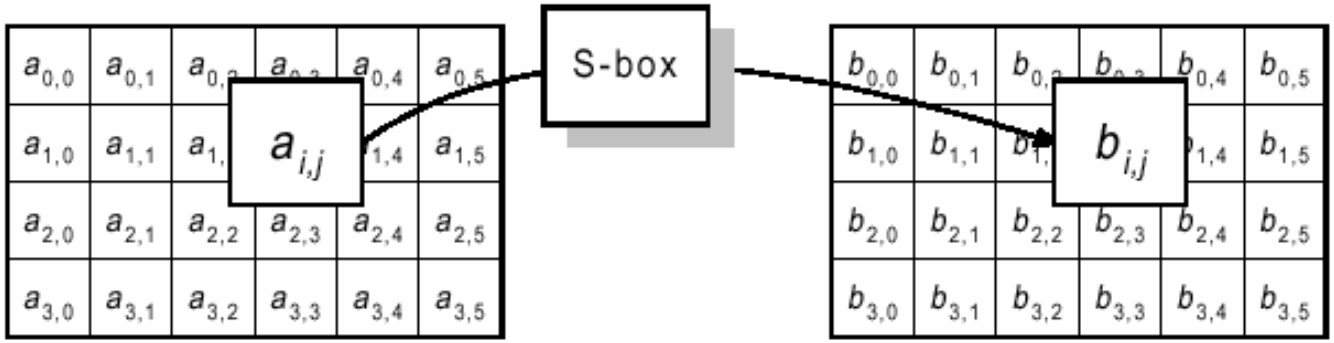
- Vast speed improvement over DES in both hardware and software implementations


Key
K
KE
Key Expansion
Round
Keys
k1
k2
k3
Kn-2
Kn-1
kn
X
r1
r2
r3
Rn-2
Rn-1
rn
Y
Encryption Rounds r1 ... rn

Rijndael Core round functions



Rijndael: ByteSub

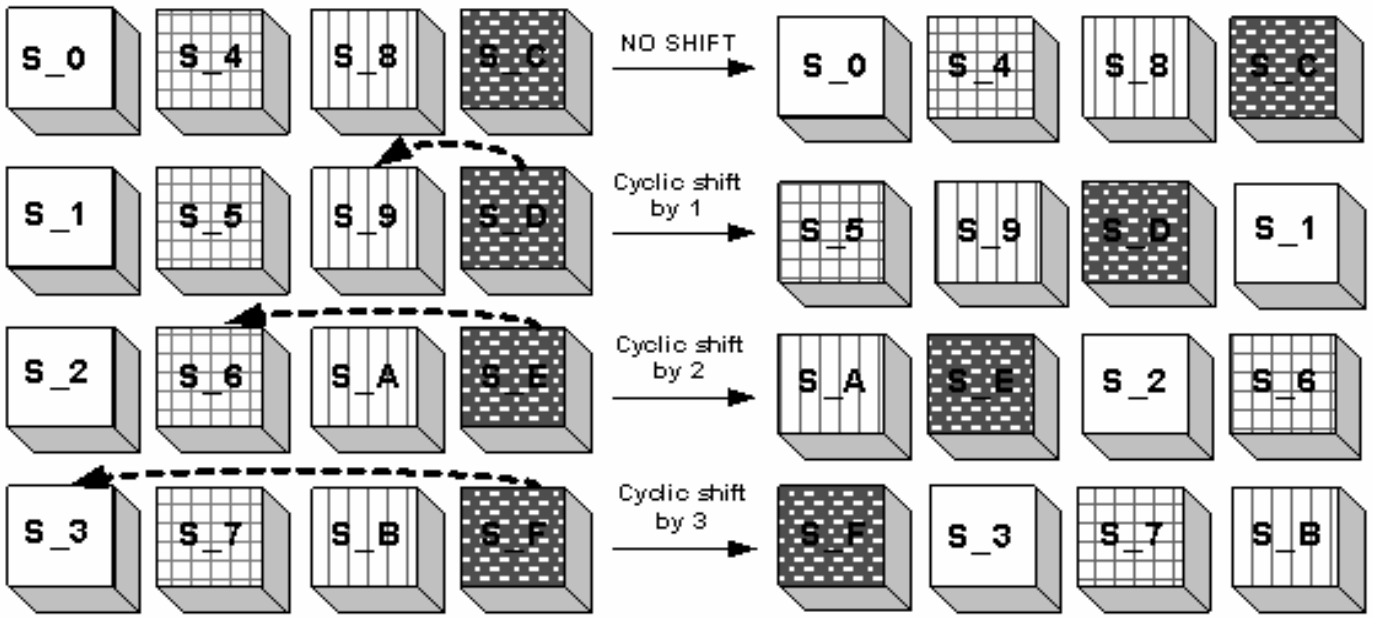


Each byte at the input of a round undergoes a non-linear byte substitution according to the following transform:

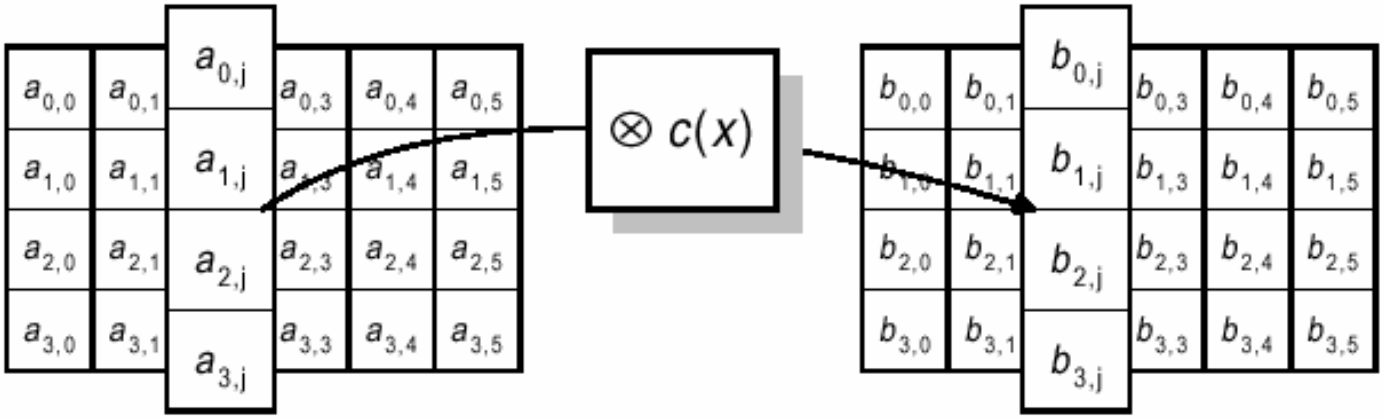
$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

[Substitution (“S”)-box]

Shift row



Rijndael: MixColumn



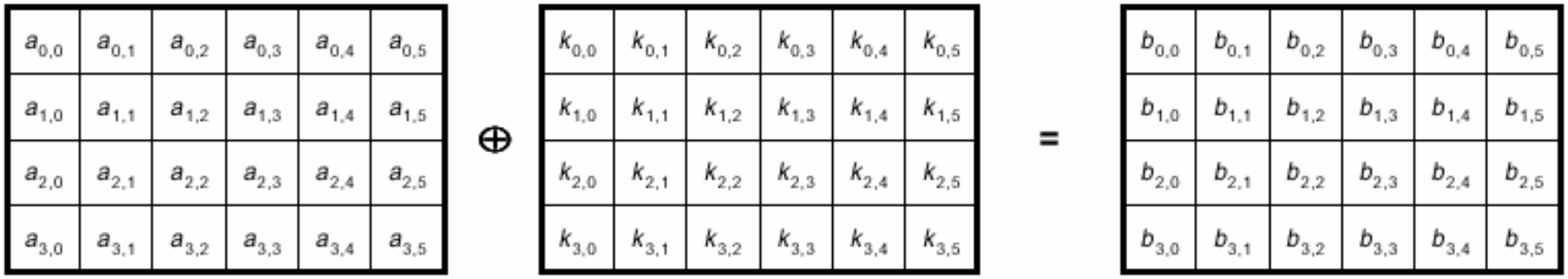
Each 4 byte column is multiplied by a fixed polynomial

C(x) = (03) . X^3 + (01) . X^2 + (01) X + (02)

This corresponds to matrix multiplication b(x) = c(x) ⊗ a(x) :

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Rijndael:
AddRoundKey



Each word is simply EXOR'ed with the expanded round key

Key Expansion algorithm see next

Rijndael includes no Involution !

Again:
No proof that AES can not be broken !!

!!! It is investigated by the international scientific community due to global open competition
We have nothing better to trust !!!!!

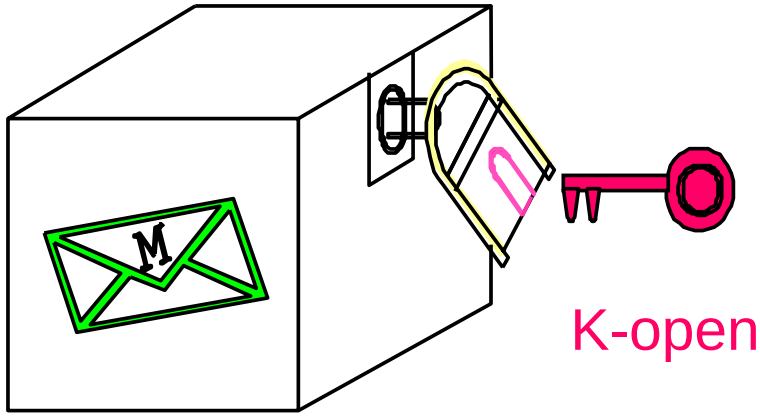
Fundamentals of

Public Key Cryptography born 1976

First introduced by Diffie and Hellmann
(Stanford University, USA)

Secret Key Cryptography

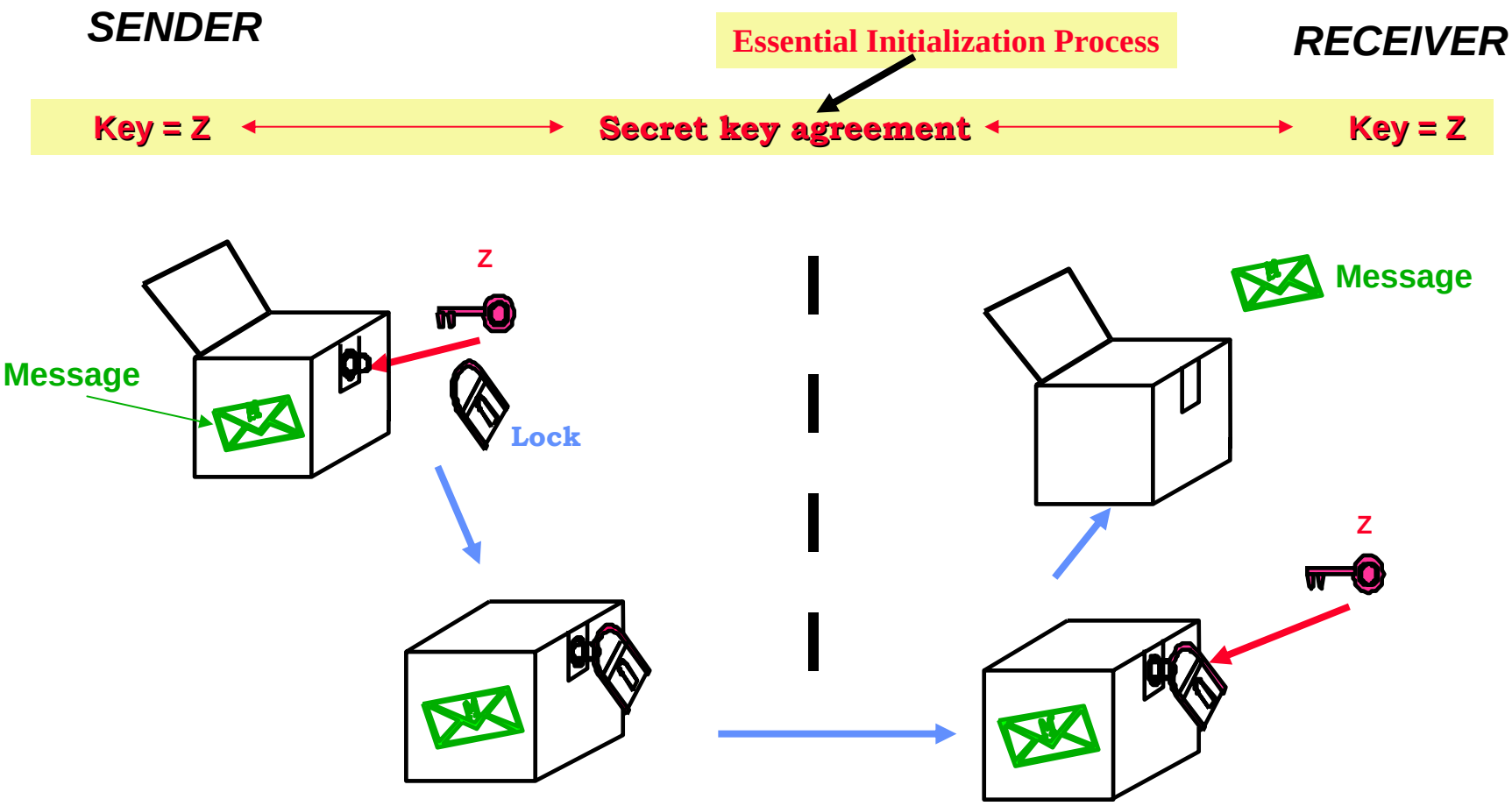
(Symmetric System)



K-open = K-close

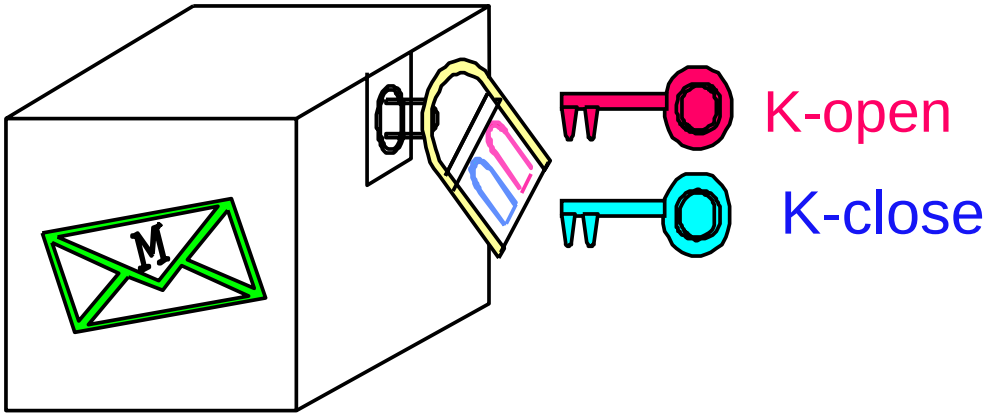
Open and close with the same key !!

Secret Key Crypto-System : mechanical analog



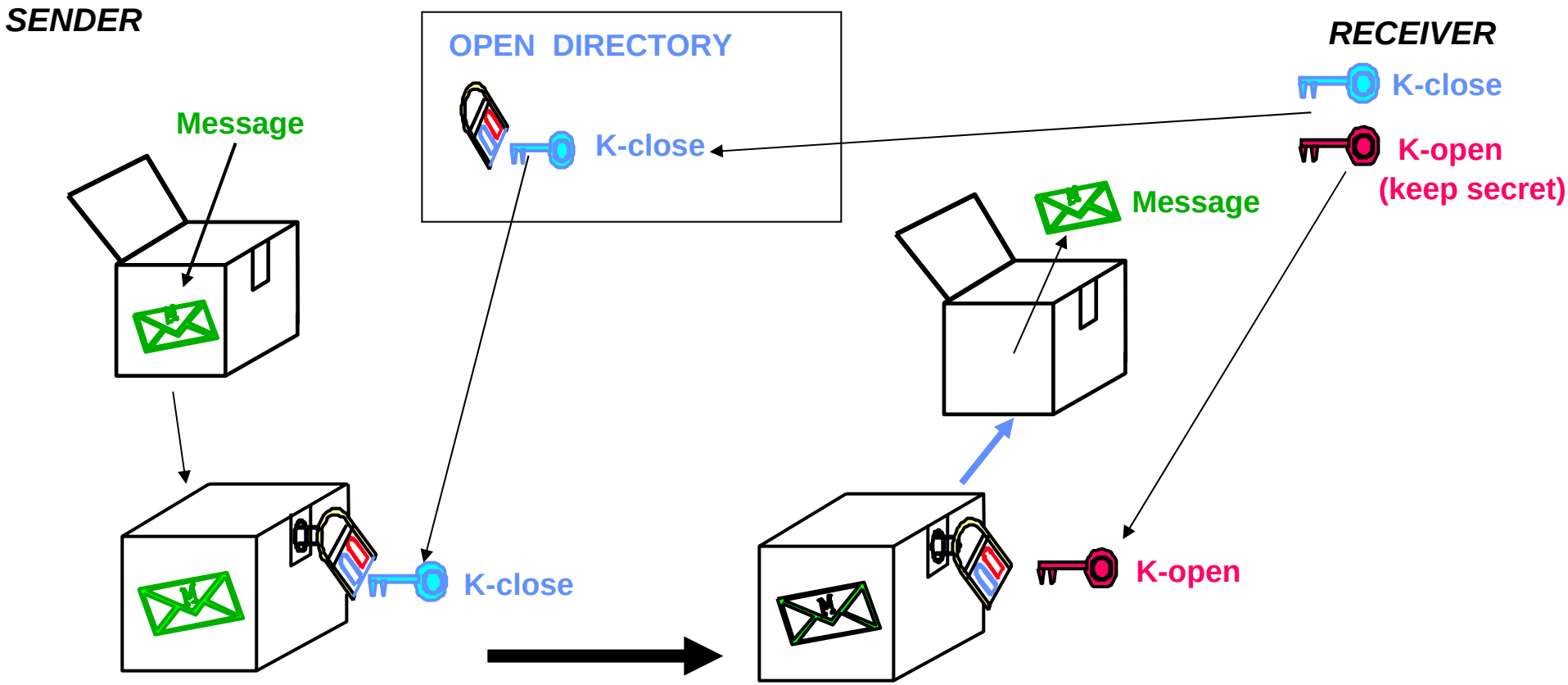
Public-Key Secrecy Systems

Diffie & Hellman 1976

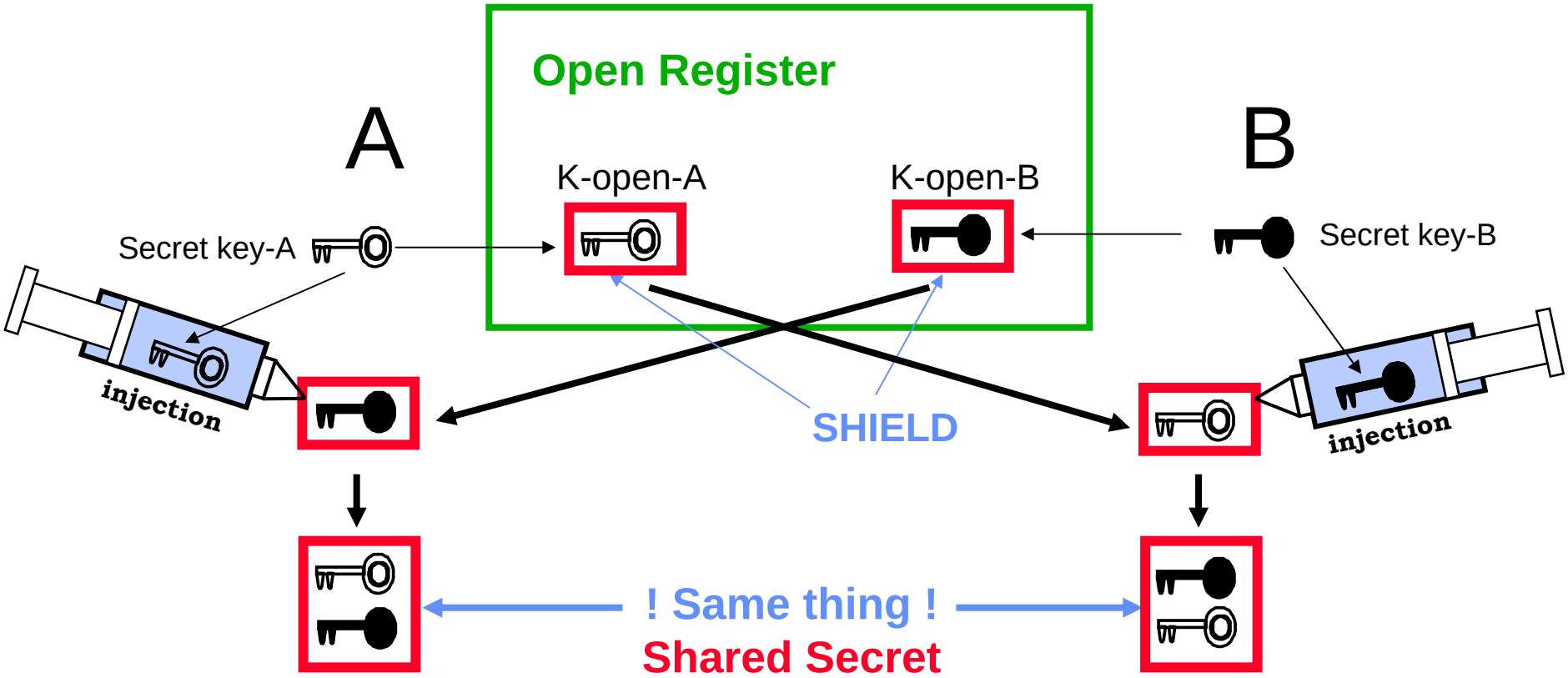


Revolutionary Invention:
to Communicate secretly without prior secret exchange

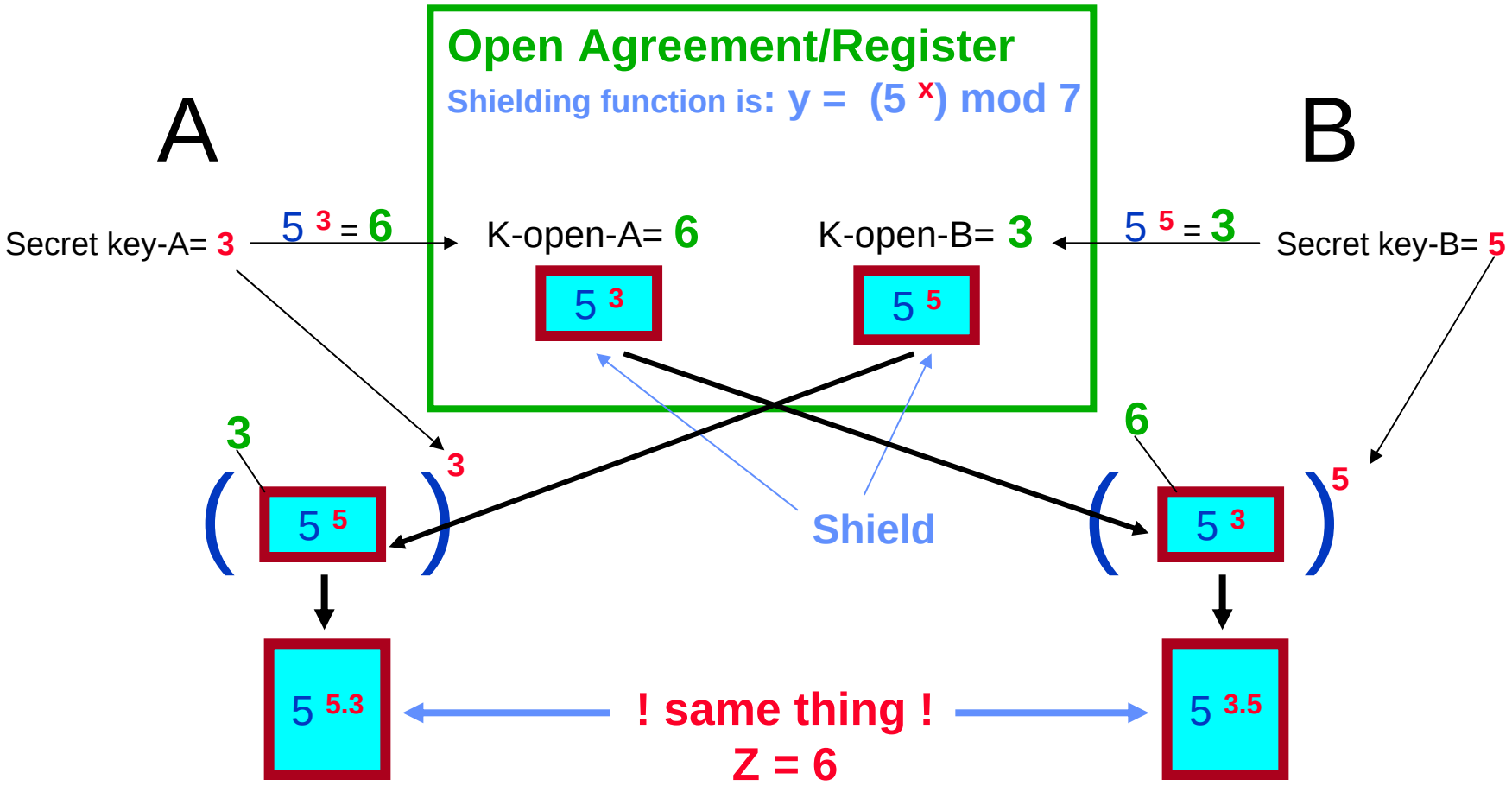
Basic public-key secrecy system : Mechanical simulation



Diffie-Hellman Secret Sharing Scheme 1976



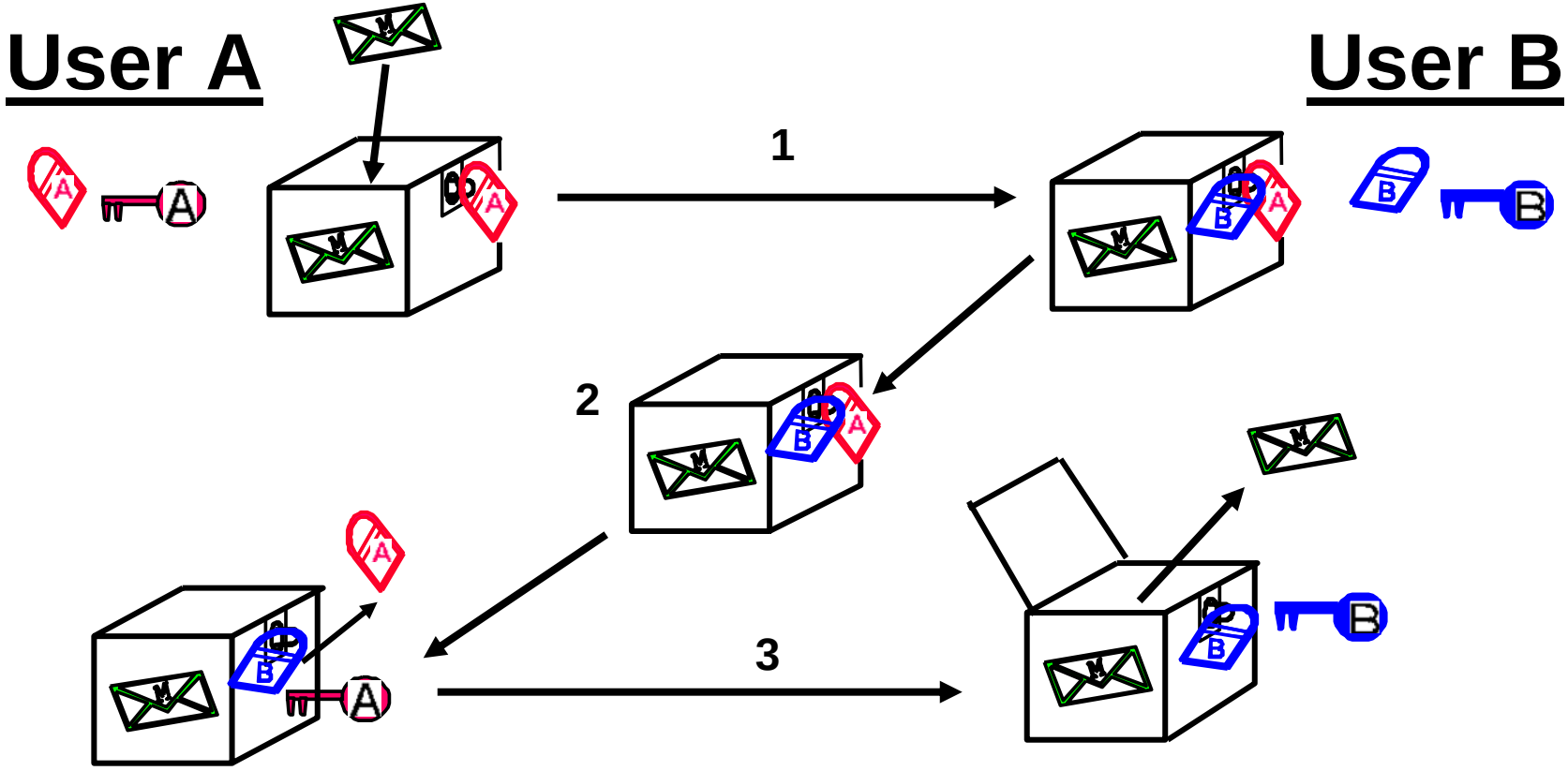
Example for *Diffie-Hellman* key exchange scheme



Cryptographic Protocols

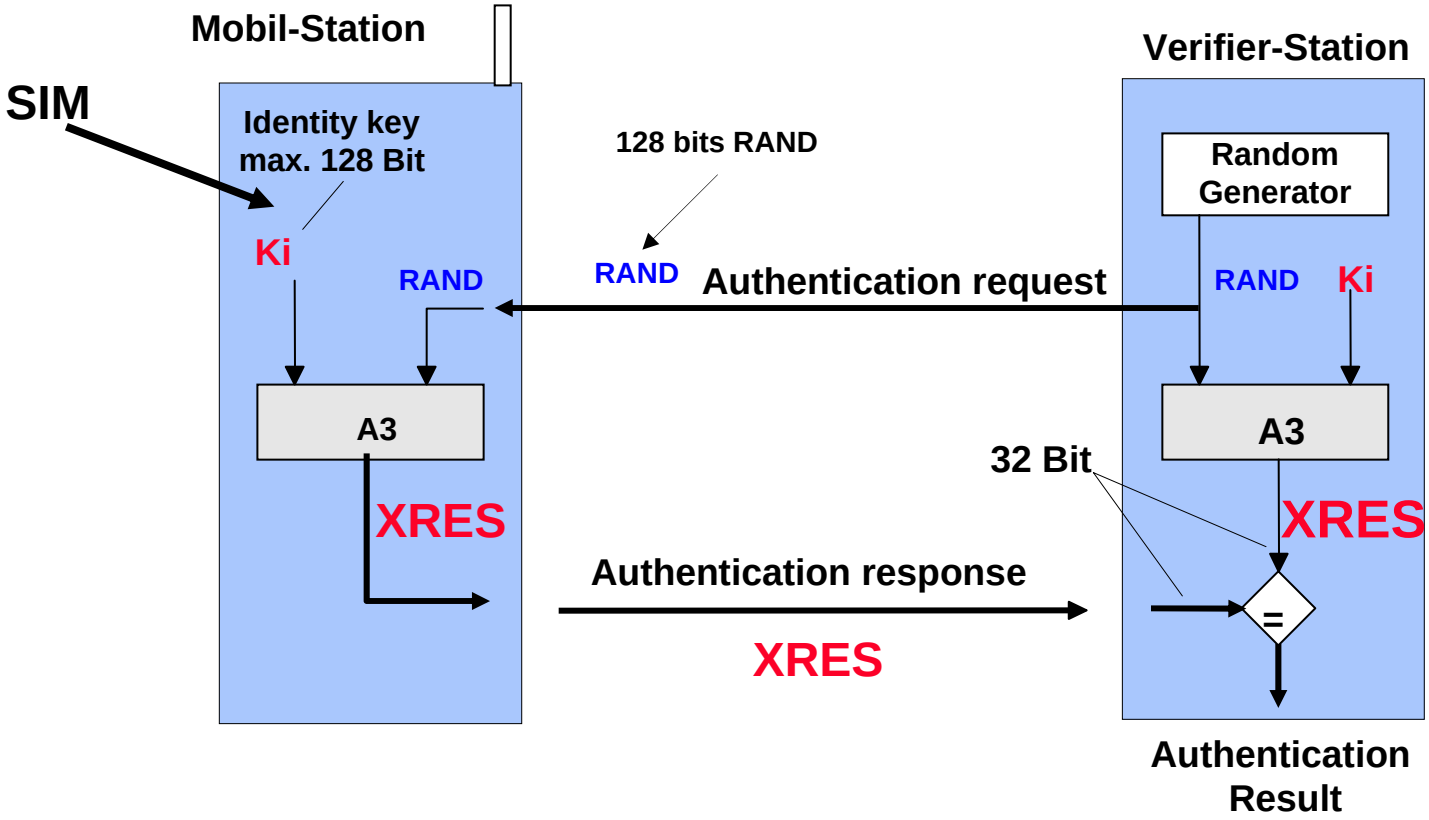
for Public Key Cryptography

Cryptographic Protocols: Shamir 3-Pass Protocol



Cryptographic Identification

GSM: Challenge-Response identification mechanism



To Conclude

No Practical *Secret Key System*

&

No *Public Key System*

has been proved to be unbreakable !

More confusing example !

Famous One-Way Functions used for Public-Key Systems

- Exponentiation $Y = a^k \pmod p$
- Multiplication in Elliptic-Curve Group

DL-Problem

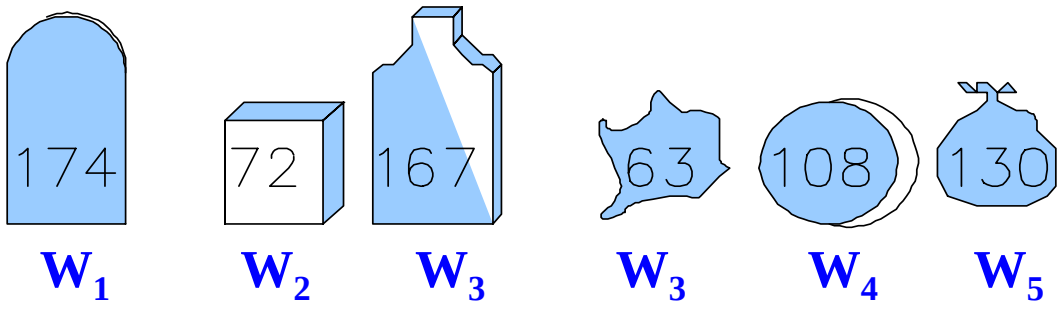
- Exponentiation $Y = M^k \pmod m$
- Factoring $m = p \cdot q$
- Squaring $C = M^2 \pmod m$

Factorizing Problem

- Knapsack Problem

$m = p.q$, p, q = large primes

Knapsack One Way Function*



Problem: Find X = [x1, x2 .....] where xi = {0,1}

Solution : ⟶ X = [1 0 1 0 1 0]

Easy if:

Superincreasing Knapsack: if W_i is more than the sum of all other smaller weights

* Ref. J. Massey

Merkle-Hellmann Crypto System (1978)

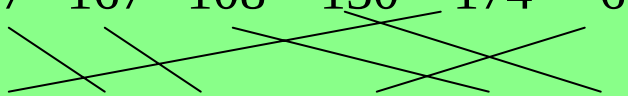
(Broken by Shamir 1984) *

1. Multiplication with $u = 113$ in Z_{199}

secret key is Z = (m, u) = (199,113)

2. Permute locations and publish

2	5	8	17	35	71	easy knapsack
27	167	108	130	174	63	hard knapsack
174	27	167	63	108	130	published knapsack



Encrypt: X = [1 0 1 0 1 0] Plaintext

Y = 174 + 167 + 108 = 449 Cryptogram

Decrypt : $Y' = u^{-1} \cdot Y = 118 \cdot 449$ in $Z_{199} = 48$

from Y´ find x´ = [0 1 1 0 1 0] in the easy knapsack

permute to get X = [1 0 1 0 1 0]

Conditions : gcd (u , m) = 1 and $m > \Sigma W_i$

* Ref. J. Massey

Can we Trust Modern IT ?

The answer is: Yes and No !

Trust Absolutely ?: No

Trust Relatively and Temporarily ? : Yes

There is no reason to hope that a new breakthrough would resolve this Dilemma in the near future !