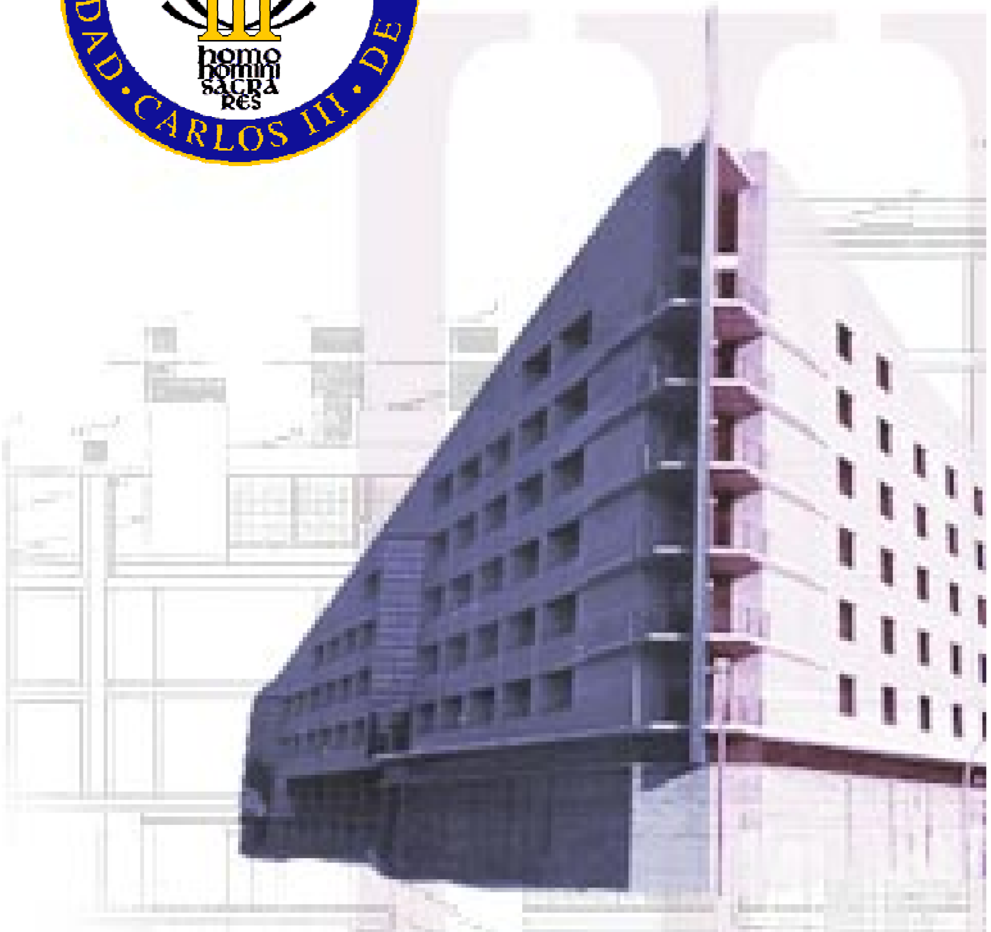


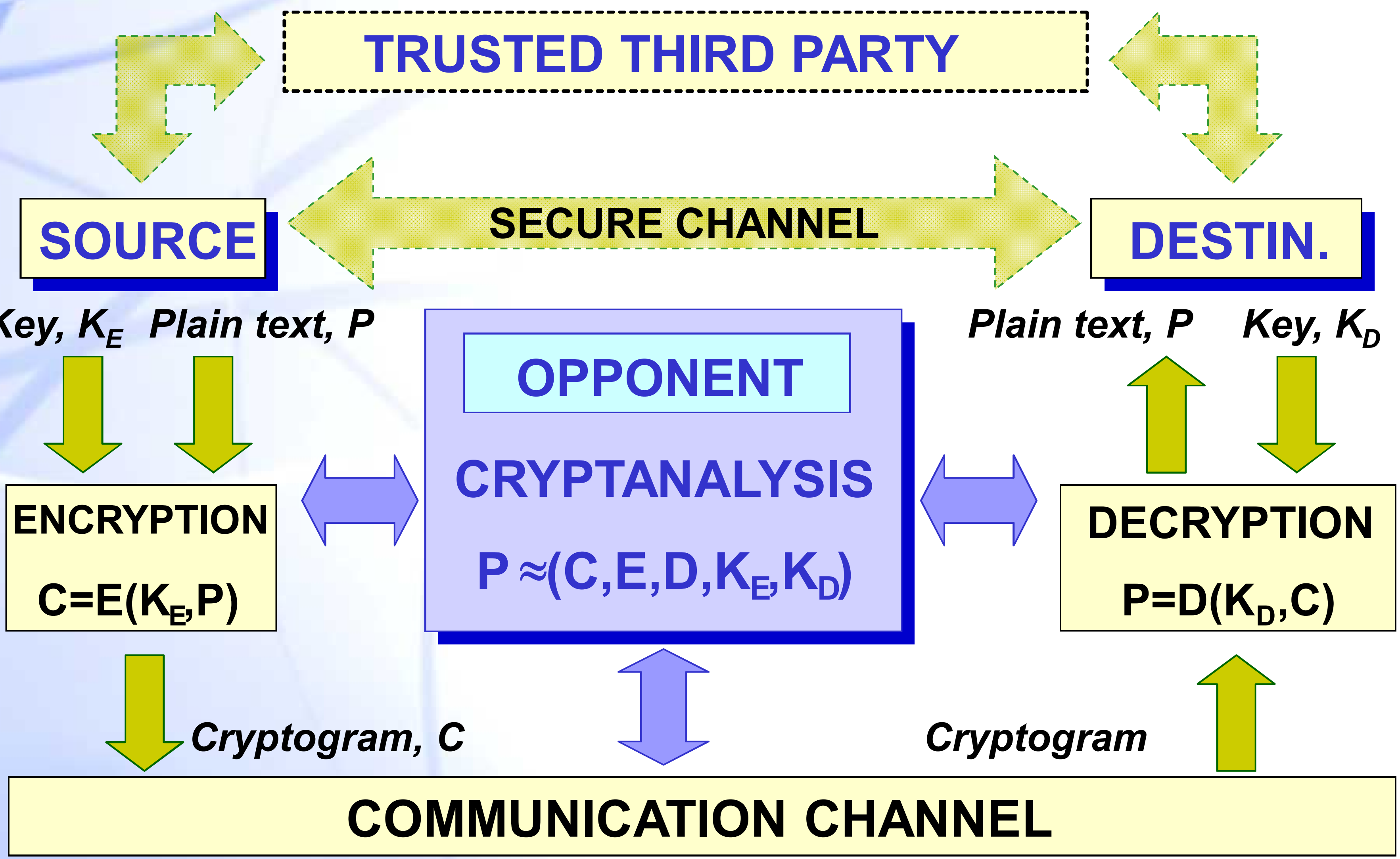
CHAPTER 3: Symmetric Cryptography

Coding Techniques

Francisco Valera Pintor

Departamento de INGENIERIA TELEMATICA
www.it.uc3m.es

CRYPTOSYSTEM MODEL



KERCHOFF'S LAW

La Cryptographie Militaire (1883 in *le Journal des Sciences Militaires*)

- **Rules a cryptosystem must comply with:**
  1. The system must be practically, if not mathematically, indecipherable;
  2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;
  3. Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents;
  4. It must be applicable to telegraphic correspondence;
  5. It must be portable, and its usage and function must not require the concourse of many people;
  6. Finally, it is necessary, seeing the circumstances that the application commands, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

SECURITY TYPES

- **Unconditional** (theoretical)
  - System is secure against attacks with unlimited resources and time
- **Computational** (practical)
  - System is secure against attacks with limited resources and time
- **Probable**
  - It has not been demonstrated that the system is insecure
- **Conditional**
  - System is secure while there are not enough resources to attack it

RSA-200 Challenge (May 2005)

The number to factorize was

**27.997.833.911.221.327.870.829.467.638.722.601.621.070.446.786.955.428.537.560.009.929.
326.128.400.107.609.345.671.052.955.360.856.061.822.351.910.951.365.788.637.105.954.48
2.006.576.775.098.580.557.613.579.098.734.950.144.178.863.178.946.295.187.237.869.221.8
23.983 (200 dígitos ~ 660 bits)**

and its prime factors are

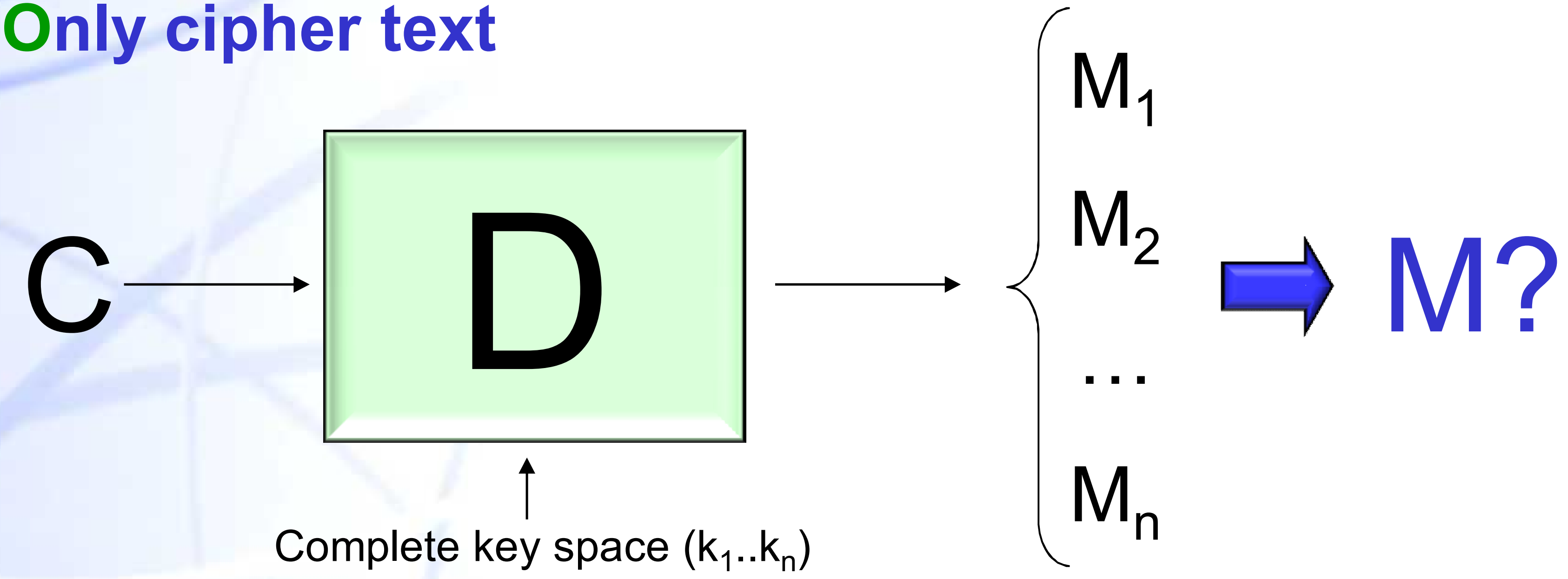
**3.532.461.934.402.770.121.272.604.978.198.464.368.671.197.400.197.625.023.649.303.468.7
76.121.253.679.423.200.058.547.956.528.088.349**

and

**7.925.869.954.478.333.033.347.085.841.480.059.687.737.975.857.364.219.960.734.330.341.4
55.767.872.818.152.135.381.409.304.740.185.467**

SECURITY ATTACKS

- **Only cipher text**



- **Cipher text and part of plain text**
- **E.g.: an 8 character ASCII text is encrypted**
  - If we decrypt with all the possible keys…
    - ✓ How many ‘M_i’ will be valid?
  - How many cryptograms are need, to obtain the encryption key

TRADITIONAL ENCRYPTION

- **Steganography**
- **Substitution techniques**
  - Monoalphabetic cipher: symbols are replaced one by one
    - ✓ Caesar cipher (1st century BC) C=(M+2) mod 26
    - ✓ General substitution C=(aM+b) mod n
    - ✓ Arbitrary substitution (Simple encryption) 26! Key space
  - Polyalphabetic cipher: substitution as function of the position
    - ✓ Vigenére encryption (1586)
    - ✓ Beaufort encryption (1710)
- **Transposition techniques**
- **Evolutionary encryption:** Vernam (1918)
- **Combined techniques:** Rotors (Scherbius 1918, Enigma 1930, etc.)

CLASSICAL CRYPTOGRAPHY

- **Substitution Techniques:**
  - Monoalphabetic cipher: symbols are replaced one-by-one
    - ✓ Caesar cipher (1st century BC) $C=(M+2) \bmod 26$
    - ✓ Linear substitution (general) $C=(aM+b) \bmod n$
    - ✓ Arbitrary substitution (Simple encryption) 26! Key space

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

V	I	N	I	V	I	D	I	V	I	N	C	I
C	C	C	C	C	C	C	C	C	C	C	C	C
X	K	P	K	X	K	F	K	X	K	P	E	K

X= (V+C) *mod* 26
23=(21+2) *mod* 26

CLASSICAL ENCRYPTION

- **Homophonic ciphers:**
  - Multiple substitutes for a single letter (homophones)
  - The more frequent, the more substitutes
  - To leverage the letter frequencies in the cryptogram
- **Multiple-letter encryption (digraphs and trigraphs)**
  - Playfair (1854): Encryption two-by-two letters
    - ✓ 5x5 encryption matrix: write a password without repeating letters and fill the matrix with the remaining letters
    - ✓ Write the letters of the plaintext in pairs. Include an 'X' between two repeated letters or at the end as padding
    - ✓ Plaintext letters in the same row are replaced by the letter to the right of each (circularly if necessary)
    - ✓ Plaintext letters in the same column are replaced by the letter beneath each (circularly if necessary)
    - ✓ Otherwise replace the letter by the letter in the same row corresponding to the column of the second letter in the pair
  - Hill (1929)

M	A	S	T	E
R	B	C	D	F
G	H	I/J	K	L
N	O	P	Q	U
V	W	X	Y	Z

PLAYFAIR EXAMPLE

M	A	S	T	E
R	B	C	D	F
G	H	I/J	K	L
N	O	P	Q	U
V	W	X	Y	Z

- **Plaintext: ELECTRONIC COMMERCE**

EL	EC	TR	ON	IC	CO	MX	ME	RC	EX
FU	SF	MD	PO	PI	BP	SV	AM	BD	SZ

- **Much better than mono-alphabetic ciphers:**
  - 26 x 26 = 676 digraphs
- **However: with a sufficiently large text, cryptanalysis is still possible**
  - Still much of the structure of the plaintext preserved

CLASSICAL CRYPTOGRAPHY

- **Polyalphabetic cipher:** Substitution as a function of their position
  - ✓ Vigenère cipher (1586): $C_i = (M_i + K_i) \ mod\ 26$
  - ✓ Beaufort cipher (1710): $C_i = (-M_i + K_i) \ mod\ 26$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

VIGENÈRE

P	E	T	E	R	L	E	G	R	A	N	D	I	S	A	G	O	O	D	F	R	I	E	N	D	O	F	N	A	P	O	L	E	O	N	L	E	G	R	A	N	D
E	D	G	A	R	E	D	G	A	R	E	D	G	A	R	E	D	G	A	R	E	D	G	A	R	E	D	G	A	R	E	D	G	A	R	E	D	G	A	R	E	D
T	H	Z	E	I	P	H	M	R	R	R	G	O	S	R	K	R	U	D	W	V	L	K	N	U	S	I	T	A	G	S	O	K	O	E	P	H	M	R	R	R	G

BEAUFORT

T	H	I	S	I	S		H	E	S	A	M	E	O	L	D	S	T		F	F
W	I	N	D	W	I		D	W	I	N	D	W	I	N	D	W	I		D	W
D	B	F	L	O	Q		W	S	Q	N	R	S	U	C	A	E	P		Y	R

T=19, -T *mod* 26=7, W=22

(-T+W) *mod* 26= 29 *mod* 26= 3 = D

(-D+W) *mod* 26= (23+22) *mod* 26= 19 = T

CLASSICAL CRYPTOGRAPHY

- **Evolutionary encryption:**
  - Vigenére's Autokey (text addition)
  - Vernam (1918): plain text XOR cyclic or pseudorandom key of the same length
  - One-time pad: XOR with random key as long as plain text
    - ✓ Unconditional security proven: no relationship between M & C
    - ✓ Key to be used only once: key distribution problem
- **Transposition techniques:** change order of symbols
  - Rail fence: rows

```
C M R I E E T O I O
 O E C O L C R N C     ⟶  CMRIEETOIOOECOLCRNC
```

  - Columns

```
Key:            4 3 1 2 5 6 7
Plain text:     a t a q u e p
                o s t p u e s
                t o h a s t a
                l a u n a a m
Cryptogram:    ATHUQPANTSOAAOTLUUSAEETAPSAM
```

  - Generic transposition: key is the pattern

ROTOR MACHINES

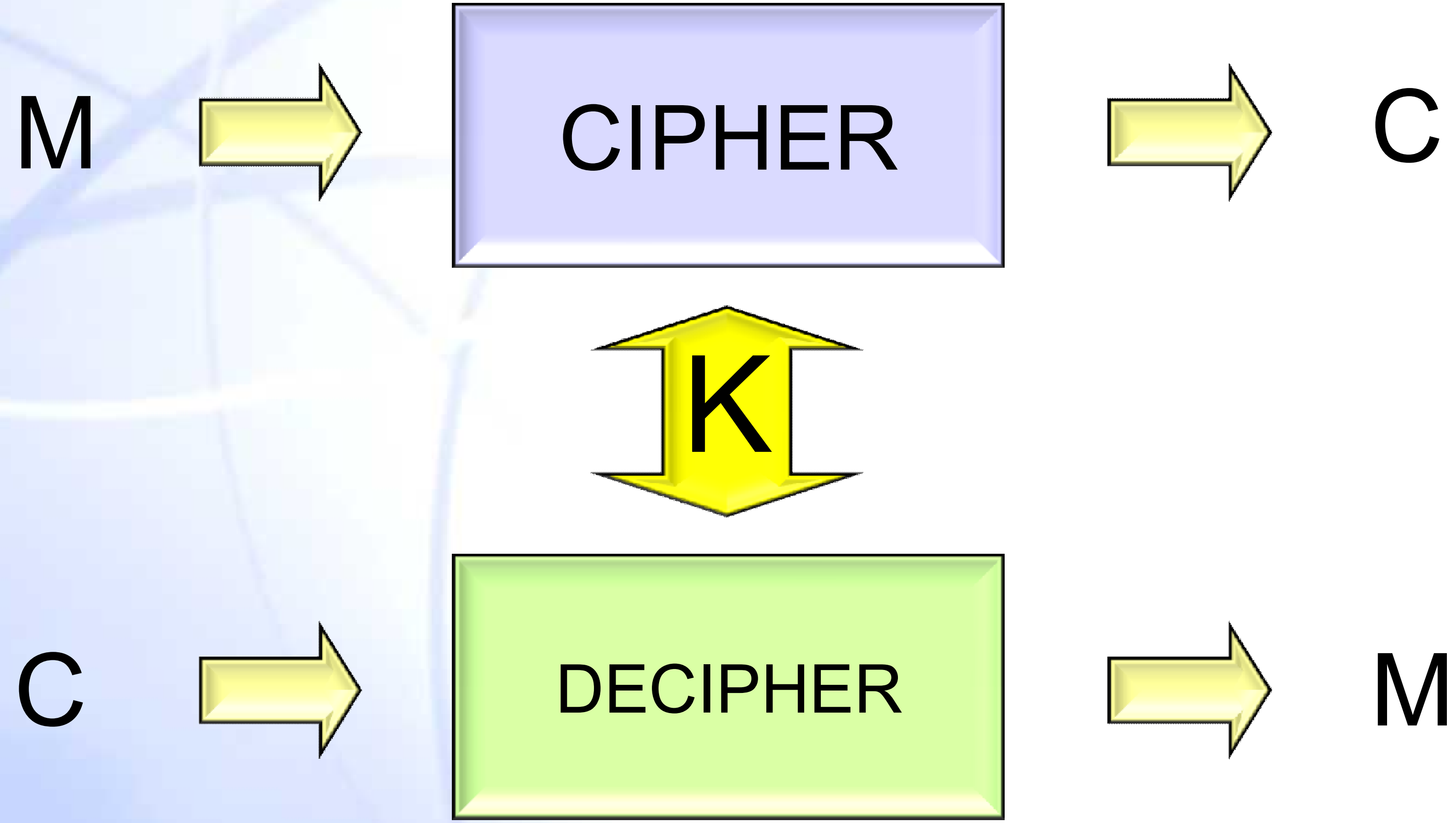
- **Electromechanic encrypters (1930-1950)**
  Enigma (Germany), Sigaba (USA), Purple and Red (Japan), Hagelin (Sweden)
- **Each cylinder constitutes a substitution cipher**
- **The output from one cylinder is the input of the following**
- **After a symbol input, the first cylinder rotates**
- **After a complete rotation of the first cylinder, the next one rotates one position**
  - A machine with ‘n’ cylinders generates a polyalphabetic cipher of period 26·n

MODERN CRYPTOGRAPHY

- **Secret Key:**
  - Symmetric encryption
    - Stream ciphers
    - Block ciphers
  - Methods of authenticating messages (MACs)
  - Mechanisms of authentication and key exchange
- **Public key:**
  - Asymmetric coding
  - Digital signatures
  - Mechanisms of authentication and key exchange
- **Without key:**
  - Hash functions

SYMMETRIC ENCRYPTION

- **Same key to encrypt and decrypt**



TYPES OF CIPHERS

- **Block Ciphers:**
  - Encoding scheme that divides the plaintext into "chunks" (blocks) of fixed size and encodes them separately

$M_1, M_2, \ldots, M_n \longrightarrow$ BLOCK CIPHER $\longrightarrow C_1, C_2, \ldots, C_n$

$K \longrightarrow$ BLOCK CIPHER

$C_i = f_K(M_i)$

- **Stream Ciphers:**
  - Encode continuous strings of bits in such a way that each operation also depends on the previous encoding

$M_1, M_2, \ldots, M_n \longrightarrow$ STREAM CIPHER (MEMORY) $\longrightarrow C_1, C_2, \ldots, C_n$

$K \longrightarrow$ STREAM CIPHER

$C_i = f_K(M_i, M_{i-1}, \ldots, M_1)$

CONFUSION AND DIFFUSION

- **Confusion:** the ciphertext depends (as complex as possible) on the key and the plaintext
  - Achieved by substitution
- **Diffusion:** message characters are mixed and redistributed in the cryptogram
  - Achieved by transposition
- **M**odern cryptosystems apply a series of rounds (iterations) to achieve both effects
  - Very complex dependency between ciphertext, key, and plaintext
  - The variation of 1 bit in the plaintext or the key results in a variation of 50% of the ciphertext (avalanche effect)

SAC: *Strict Avalanche Criterion*

RANDOM SUBSTITUTION

- **The security provided by random substitution mechanisms should be enough**
  - For an ‘s’ symbol ordered alphabet, there are s! ways to change their order (possible bijections)
  - The key are the ‘s’ symbols reordered

4 symbol alphabet

00
01
10
11

24 possible orders →

01
10
11
00

→ **The order would be the selected key** $\boxed{01101100}$

- If we have an ‘n’ bits block, there would be 2^n symbols in the alphabet and the key size would be $n \cdot 2^n$ bits
- For n=64 bits the key would be around 10^{21} bits

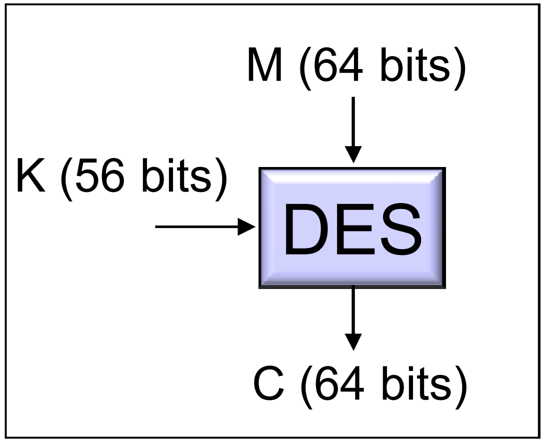
- **Solution: product ciphers combine simple substitution and transposition**

SYMMETRIC ENCRYPTION: DES

National Bureau of Standards, ahora NIST: National Institute of Standards and Technology

- Origin: US NBS competition (1973)
- Winner: "Lucifer" algorithm of IBM (1975)
- Adopted in 1977 (FIPS46) until 1998 (FIPS46-3)
- Weakness: the length of the key.
  - 1977: 20 million $ to break it in 24 hours
  - 1993: 1 million $ to break it in 3 hours
  - 1997: 1st RSA challenge (96 days)
  - 1998: EFF (210.000 $), 56 hours
  - 1999: DesCrack, 22 hours
  - AES1 (1998), AES2 (1999), AES3 (2000)
  - 2001: Rijndael (AES-FIPS197) official subtitute for DES
  - 2004: the withdrawal of FIPS46-3 is proposed

DES PROPERTIES



- **Block cipher**
- **Only hardware until 1981**
  - DEA (Data Encryption Algorithm)
  - ANSI X9.32
- **Block size = 64 bits**
- **Key size = 56 bits**
- **Avalanche effect 50%**
- **Weak keys (4)** ⇨ $E_{kd}[E_{kd}(M)]=M$
- **Semi-weak keys (12)** ⇨ $E_{ks2}[E_{ks1}(M)]=M$

ENCRYPTION EXAMPLE

PLAIN TEXT

secretos

ASCII Coding

115 101 99 114 101 116 111 115

ASCII CODING IN HEXADECIMAL

73 65 63 72 65 74 6f 73

ASCII KEY IN HEXADECIMAL

'KEYONE': 63 6c 61 76 65 75 6e 6f

ASCII CODING IN BINARY

01110011 01100101
01100011 01110010
01100101 01110100
01101111 01110011

DES

01111100 11010010
00011111 11001010
10000001 11111100
00100010 11000010

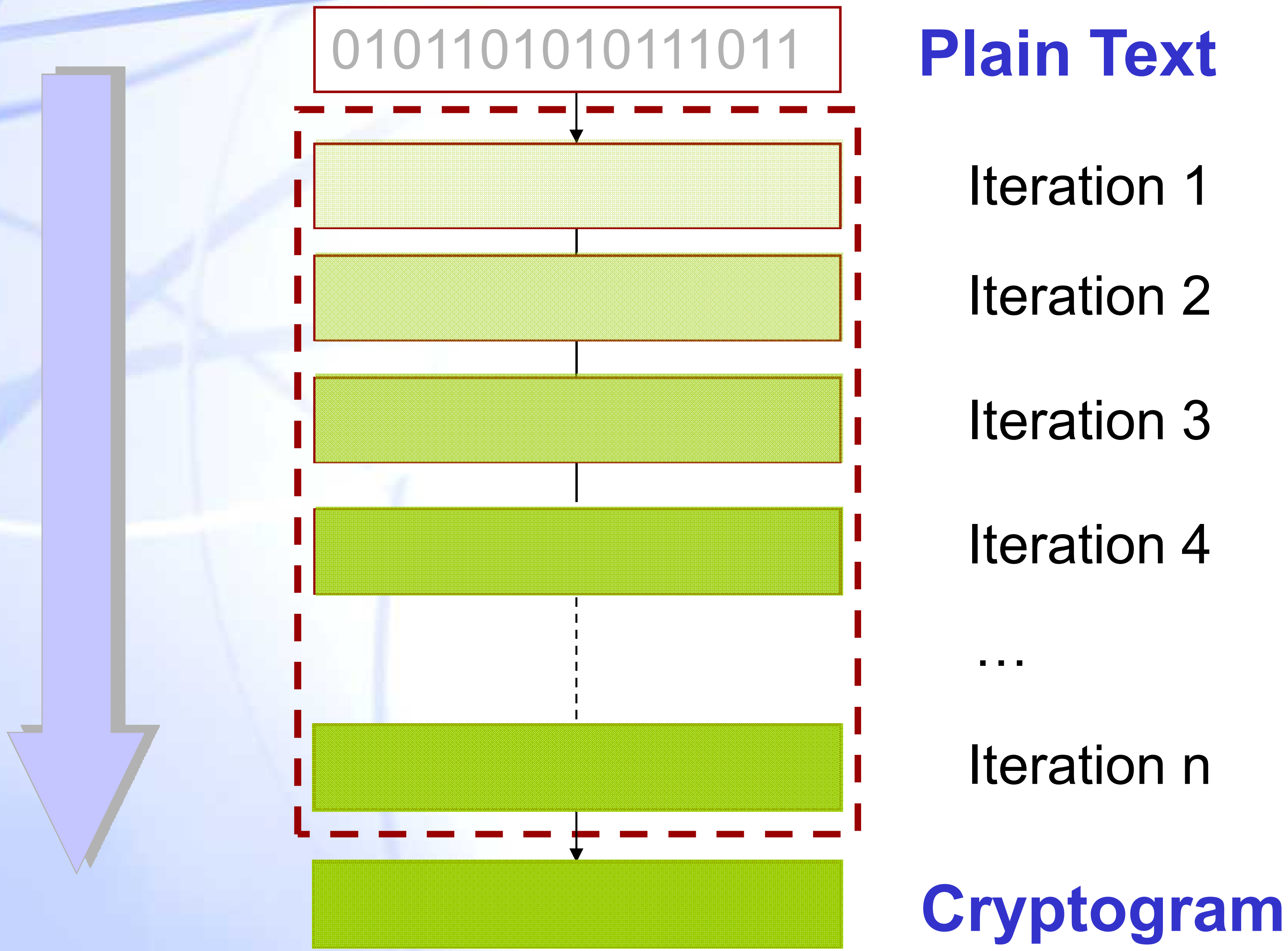
7c d2 1f ca 81 fc 22 c2

124 210 31 202 129 252 34 194

ENCRYPTED TEXT

|ÒÊü"Â

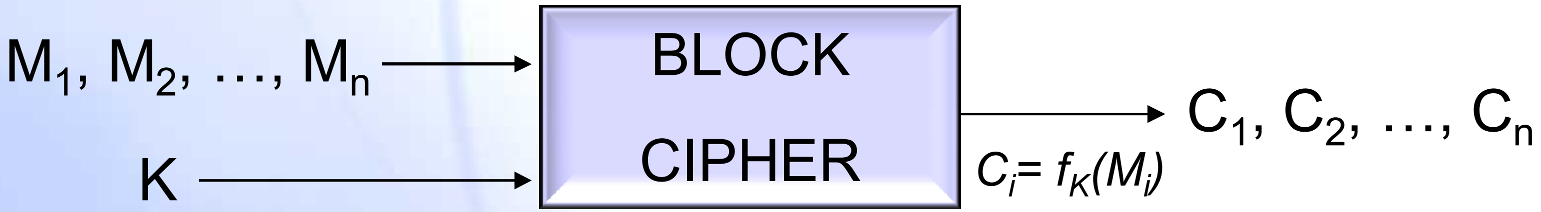
DES ITERATIONS



MODES OF OPERATION

◆ Block Ciphers

- Coding scheme that divides the plaintext into ‘chunks’ (blocks) of fixed size and encodes them independently
- Easier to perform than stream ciphers
- If the size of the data to encode is less than the block size ⇨ padding
- If the size of the data to encode is greater than the block size ⇨ modes of operation



PADDING

- **The padding mechanism is not exclusive from encryption algorithms**
  - E.g.: Ethernet has to align the frame, etc.
- **Introduces redundancy**
  - It must have a known format so that the destination can delete it
- **Decreases encryption performance**
  - Plain text / Cipher text relation
- **It is necessary**
  - If it is not used the destination has to wait in order to receive more bits so as to complete the whole block

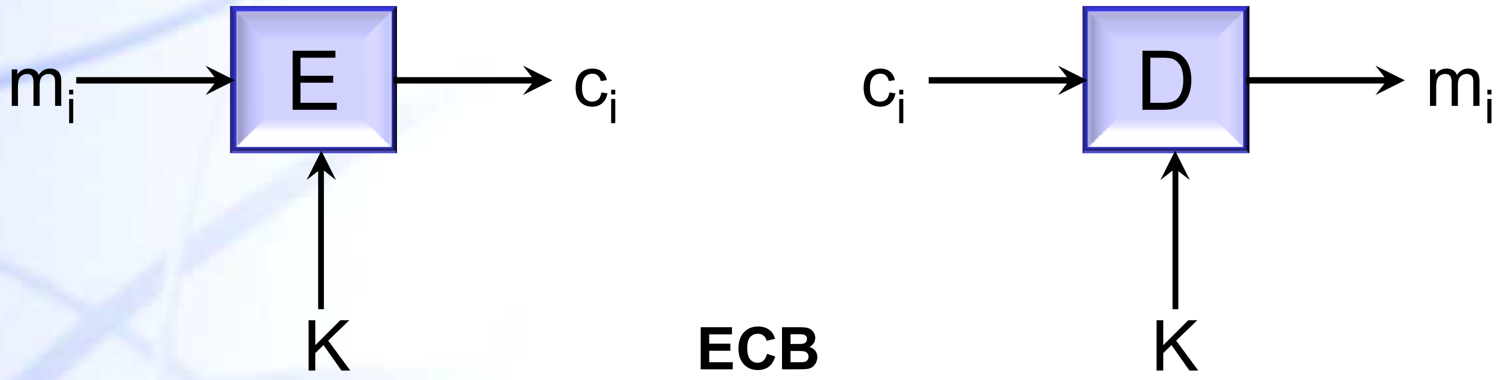
PADDING

- **Padding examples:**
  - Add a known data tail (fill with ‘1’ or with ‘0’ or with a sequence of ‘0’ and ‘1’, etc.)
  - Problem: what happens if the plain text looks like the padding?
- **PKCS#5 (RFC2630, section 6.3)**
  - The padding is done with the required bytes, and their value is the binary representation of the number of added bytes
  - Problem: what happens if the plain text does not need padding and contains a substring that looks like padding?

MODES OF OPERATION

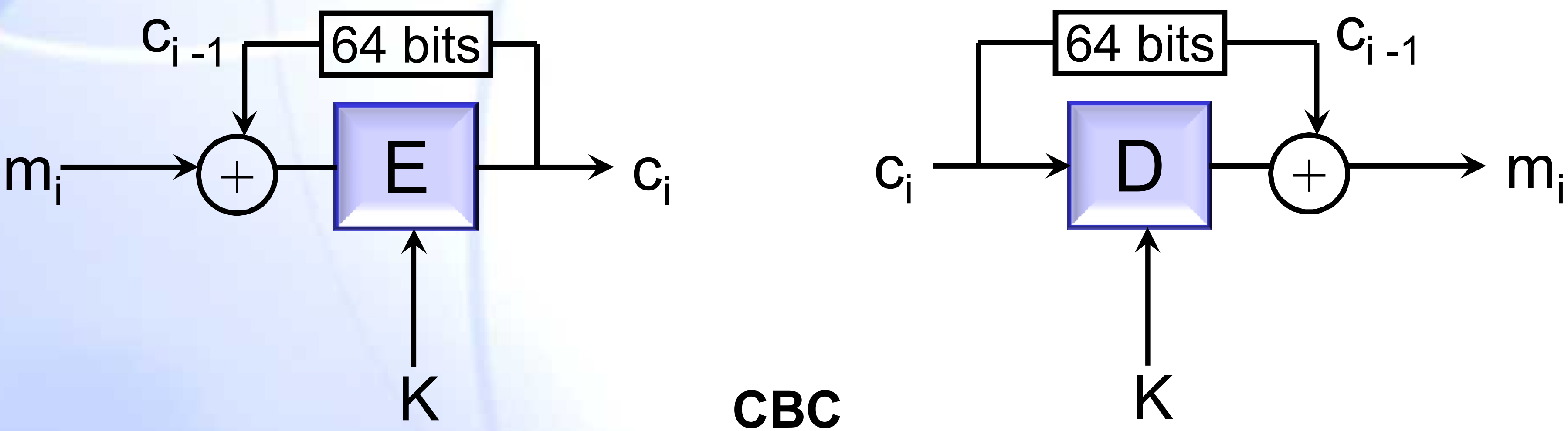
1. **Electronic Codebook (ECB)**
   - ✓ For transmission of small amounts of data without structural regularities
2. **Cipher Block Chaining (CBC)**
   - ✓ For block-oriented transmission of data
3. **Cipher Feedback (CFB)**
   - ✓ For transmission of continuous bit streams
   - ✓ Propagates bit errors
4. **Output Feedback (OFB)**
   - ✓ For transmission of continuous bit streams
   - ✓ Useful in a noisy channel (No propagation of bit errors)
   - ✓ Higher risk for message modification attack

MODES OF OPERATION



ECB

(*Electronic CodeBook Mode*)



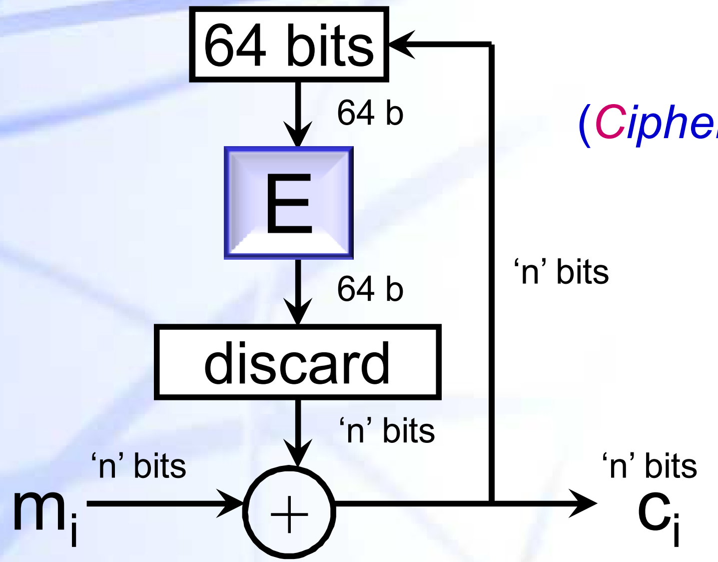
CBC

(*Cipher Block Chaining Mode*)

ECB, CBC

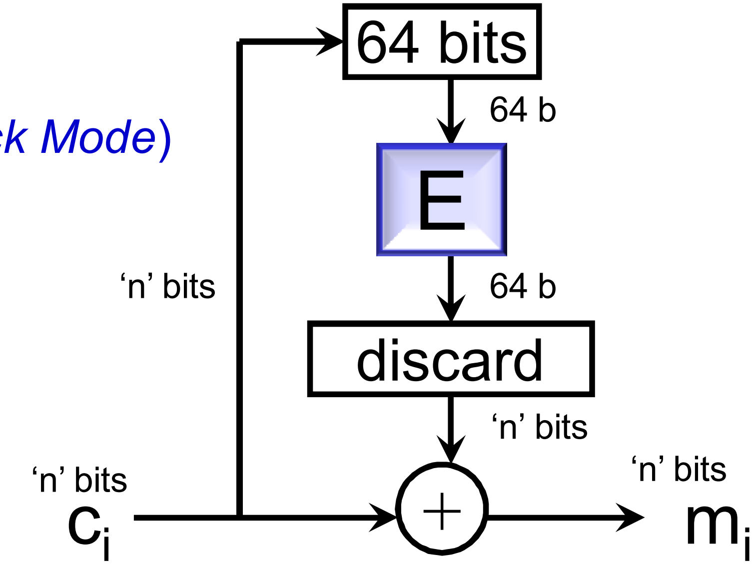
- **ECB**
  - Direct use of the algorithm as block cipher
  - Useful for small messages
  - One bit error is propagated to one full block
- **CBC**
  - Requires an initialization vector (C_0 o IV)
  - Chains the coding of different blocks
    - ✓ Identical blocks result in different ciphered blocks
  - Error propagation to one additional block
  - Self-synchronization
    - ✓ Alteration or loss of blocks

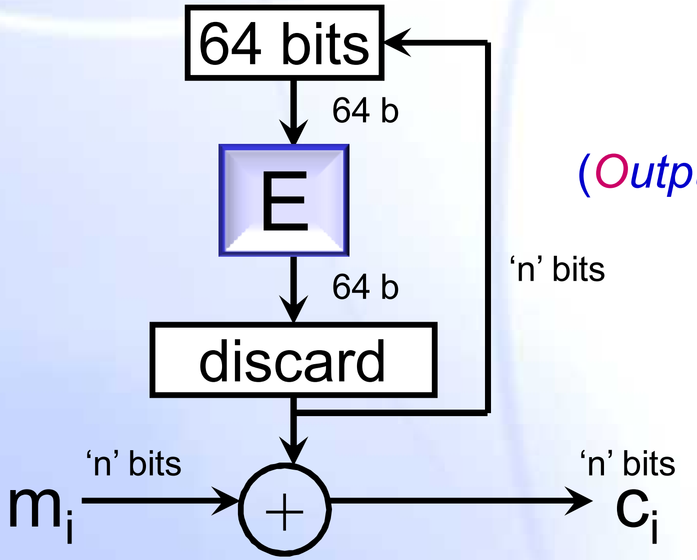
MODES OF OPERATION



CFB

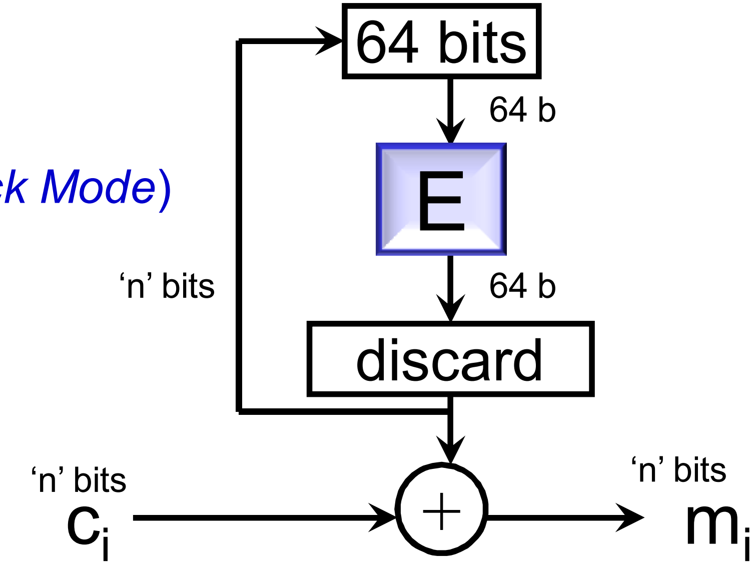
(*Cipher FeedBack Mode*)





OFB

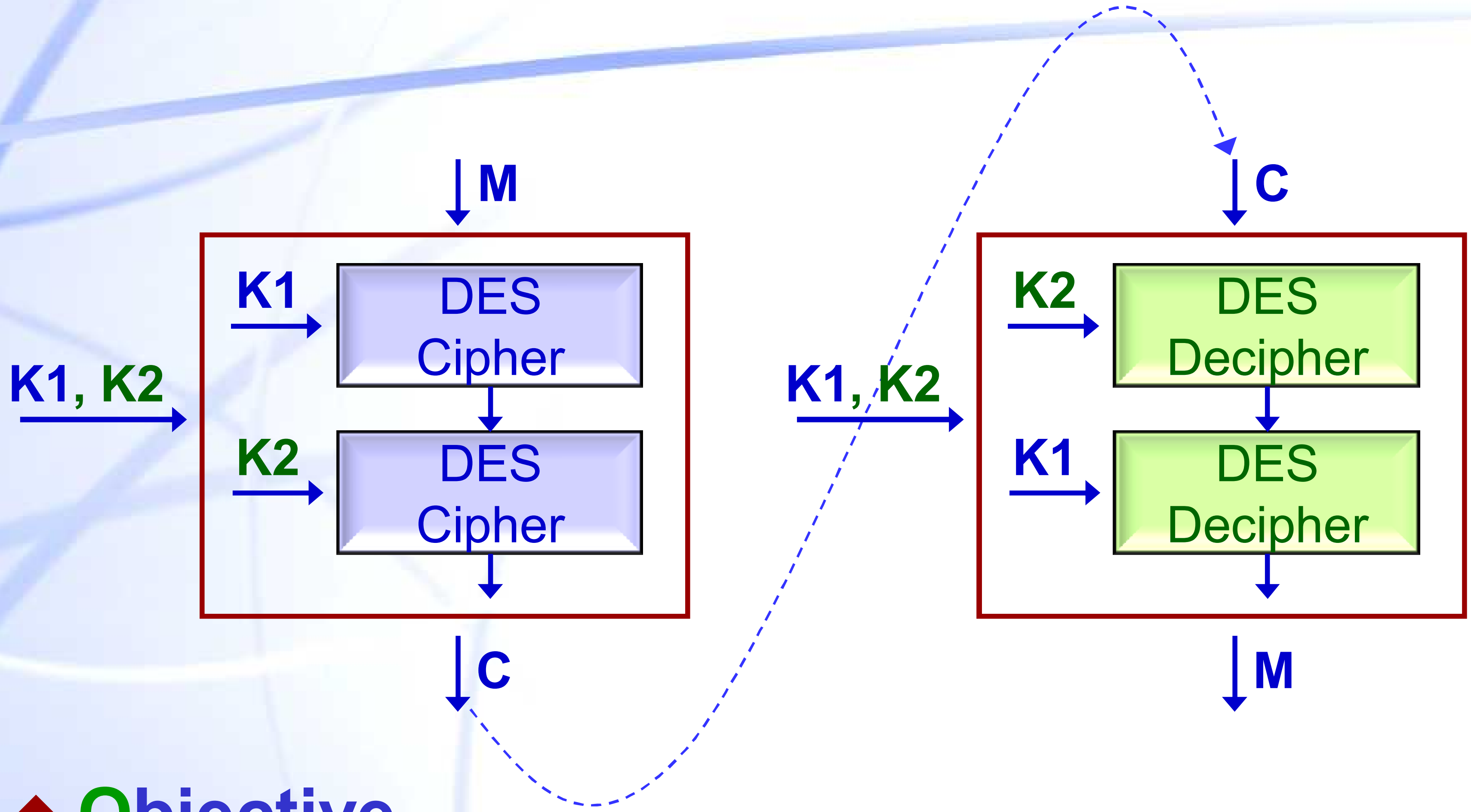
(*Output FeedBack Mode*)



CFB, OFB

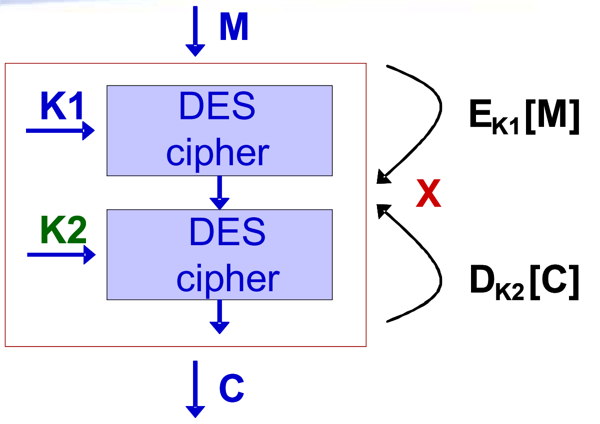
- **CFB**
  - Variable block size (multiple of 8)
    - ✓ Most similar to a stream cipher
  - Less coding efficiency
    - ✓ Eg: n=8 ⇨ each byte requires a cipher operation
  - Error propagation to one 64 bit block
  - Self-synchronizing:
    - ✓ Modification or loss of blocks
- **OFB**
  - The coder and decoder are identical
  - The algorithm is used as a pseudo-random sequence generator (can be done offline)
  - No error propagation
  - No self-synchronization on block losses

DOUBLE DES



- **Objective**
  - Increase the effective size of the key by using DES several times in succession.

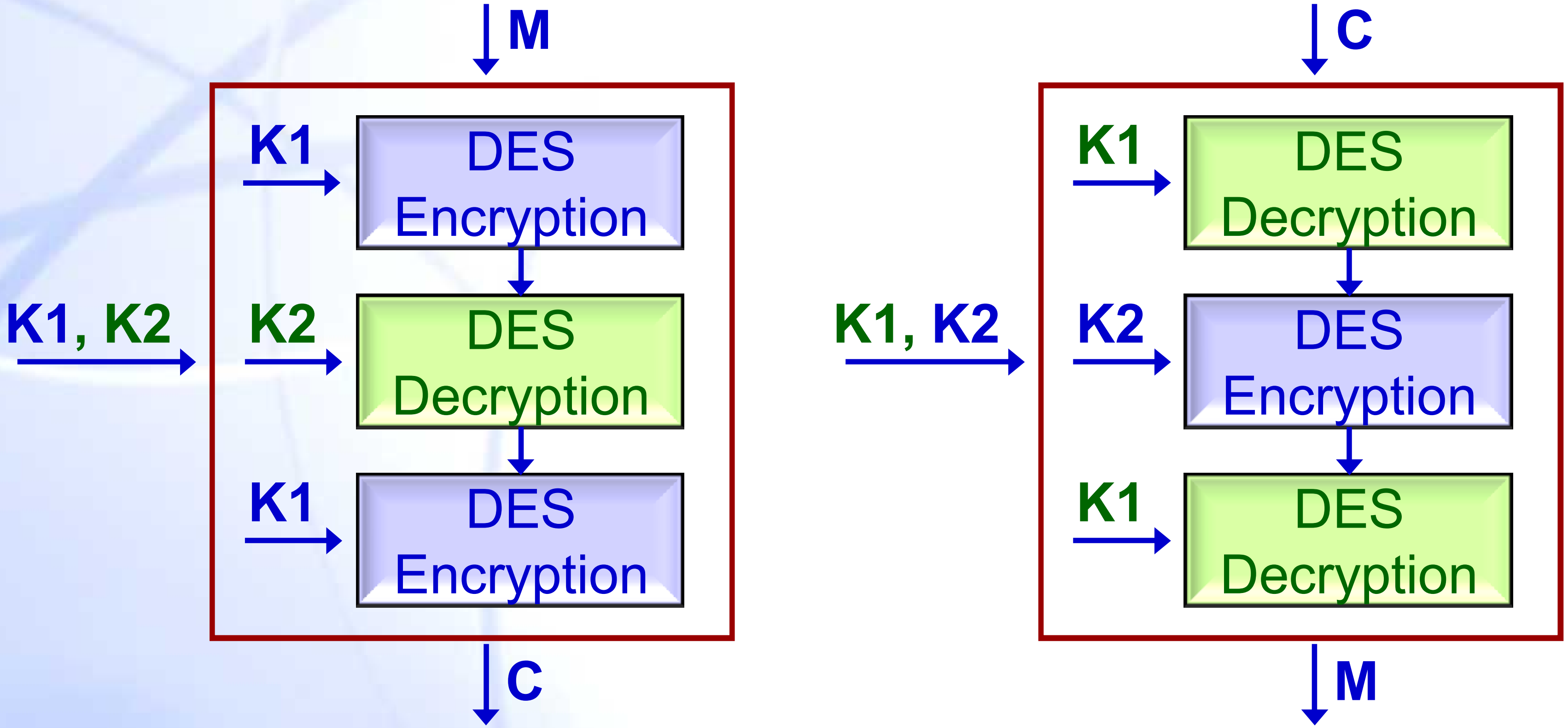
DOUBLE DES



- **'Meet-in-the-middle' attack**
  - $X=E_{K1}[M]=D_{K2}[C]$
  - Obtain a pair M/C
  - Encrypt M with the 2^{56} possible K_1 and decrypt C with the 2^{56} possibles K_2
    - ✓ Will there be coincidences?
    - ✓ There are 2^{112} possible keys and only 2^{64} outputs
      - ➢ Given a pair M/C, the number of key pairs that verify $C=E_{K2}[E_{K1}[M]]$ may be $2^{112}/2^{64} = 2^{48}$
  - Capture another M'/C' pair. The false alarm ratio is reduced to $2^{48}/2^{64} = 1/2^{16}$
  - Effective key size: 2^{57}

TRIPLE DES (TUCHMAN 79)

- DES compatibility (K=K1=K2)



THE NEW STANDARD

- DES has not been cryptanalyzed completely
- Weakness: key length (brute-force)
  - 1977: 20 $million for cracking it in 24 hours
  - 1993: 1 $million for cracking it in 3 hours
  - 1997: 1st challenge (96 days) DESCHALL
  - 1998: 2nd challenge.(56 hours) EFF ($210.000)
  - 1998: AES1 initiated (TDES already recommended)
  - 1999: 3rd challenge (22 hours) DesCrack
  - AES2 (1999), AES3 (2000)
  - 2001: **Rijndael** (AES-FIPS197) officially replaces DES
  - 2004: FIPS46-3 proposed to be withdrawn

AES: Rijndael

- AES (Advanced Encryption Standard) in 2001
- Creators: Vincent Rijmen & Joan Daemen
- Design criteria:
  - ✓ Simplicity, speed, security
- 128 bit blocks and 128, 192, and 256 bits keys
- Iteration:
  - Add Round Key: XOR of the iteration subkey
  - Byte Sub: Substitution of each byte of a block
  - Shift Row: Displacement of rows
  - Mix Column: Reordering of columns
- Number of iterations dependent on key size 10, 12, or 14 iterations

ARK

BSB
SR
MC
ARK

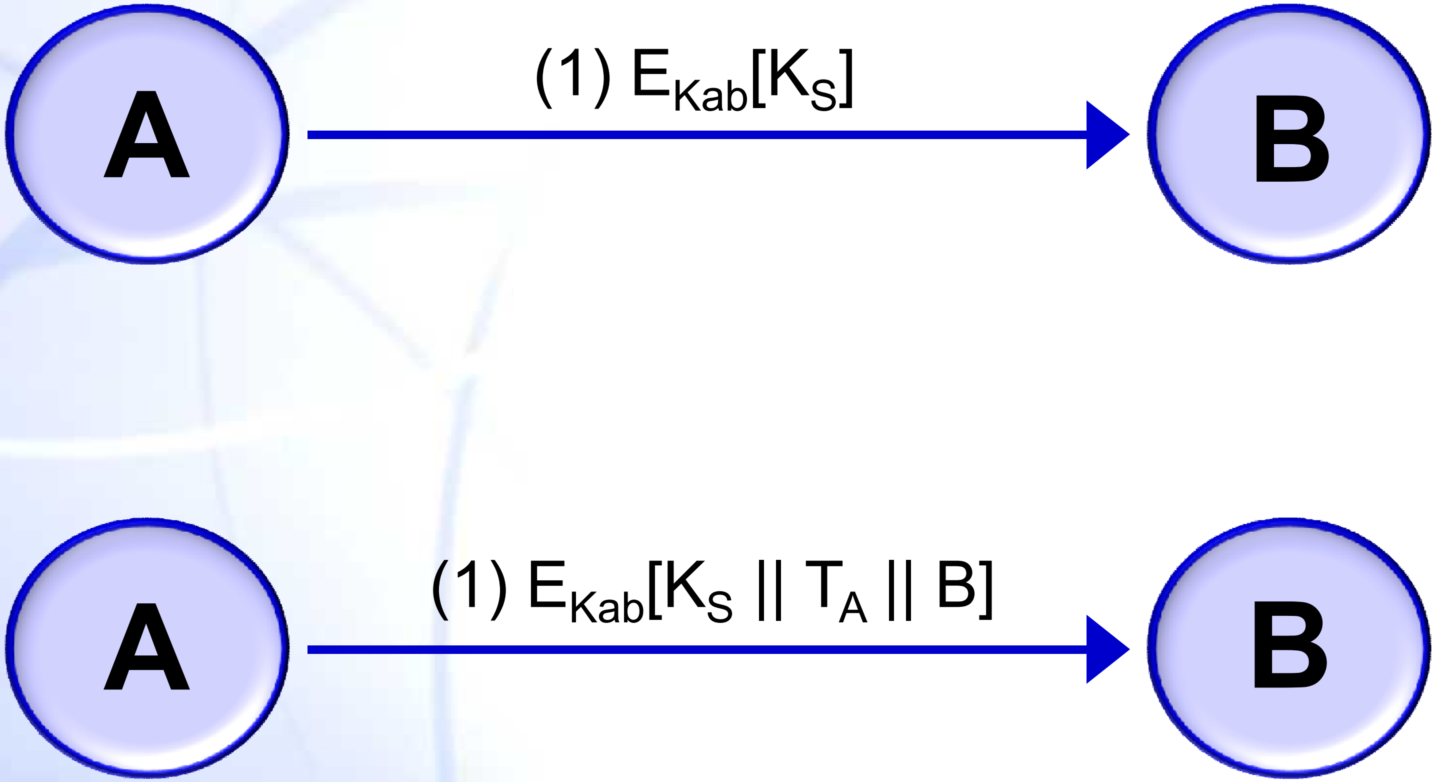
...

BSB
SR
ARK

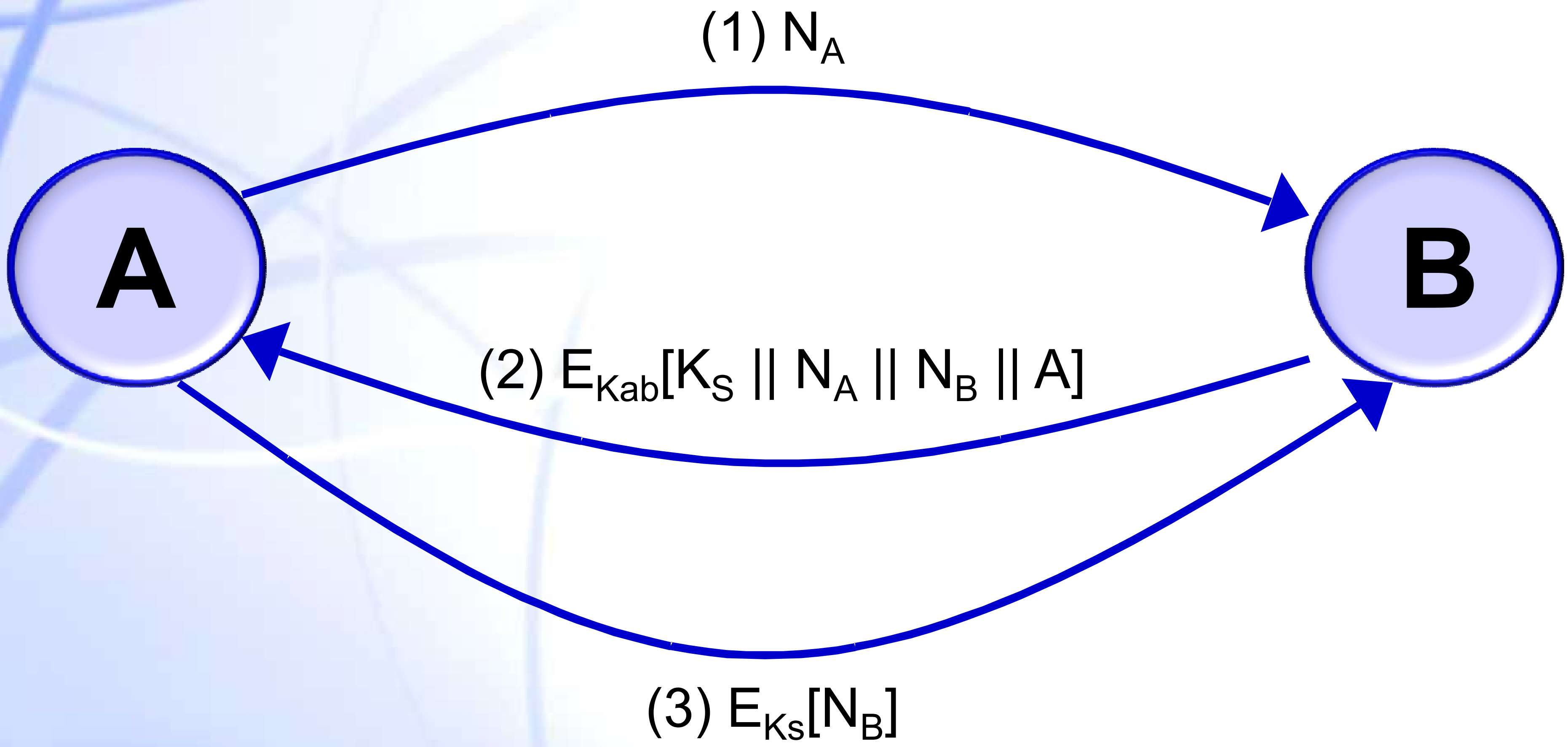
KEY DISTRIBUTION

- **Physical delivery**
  - Secure, but of relative usefulness
- **Using an old key**
  - $E_{Ks}[K_{s+1}]$
  - Capture one of the keys and the system is broken
- **Using a specific key**
  - An additional protocol must protect the distribution
- **Trusted third party**
  - Complicates the distribution mechanism

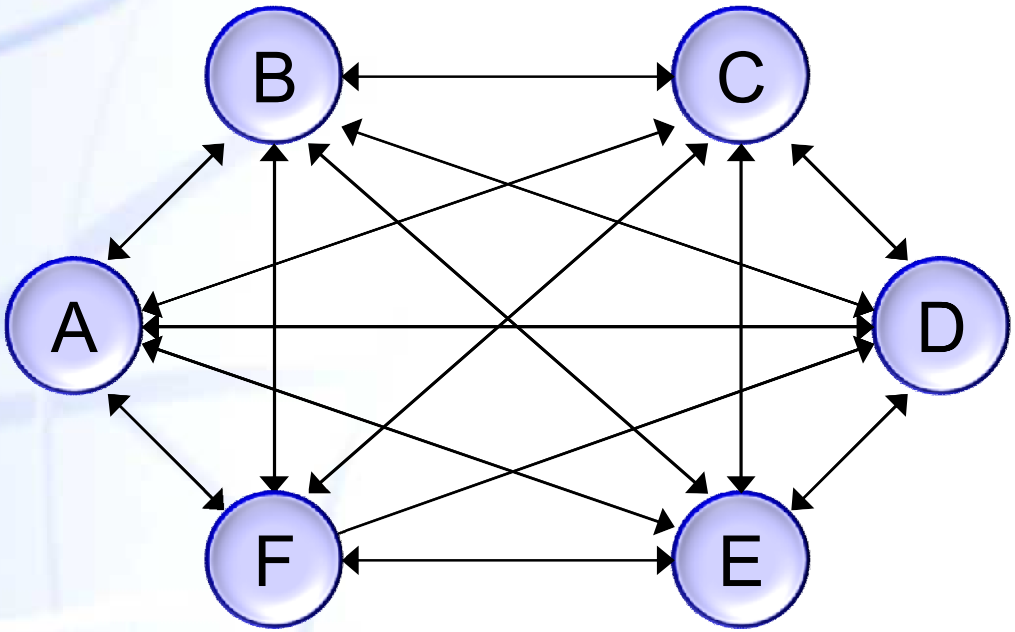
DIRECT EXCHANGE



DIRECT EXCHANGE



KEY DISTRIBUTION

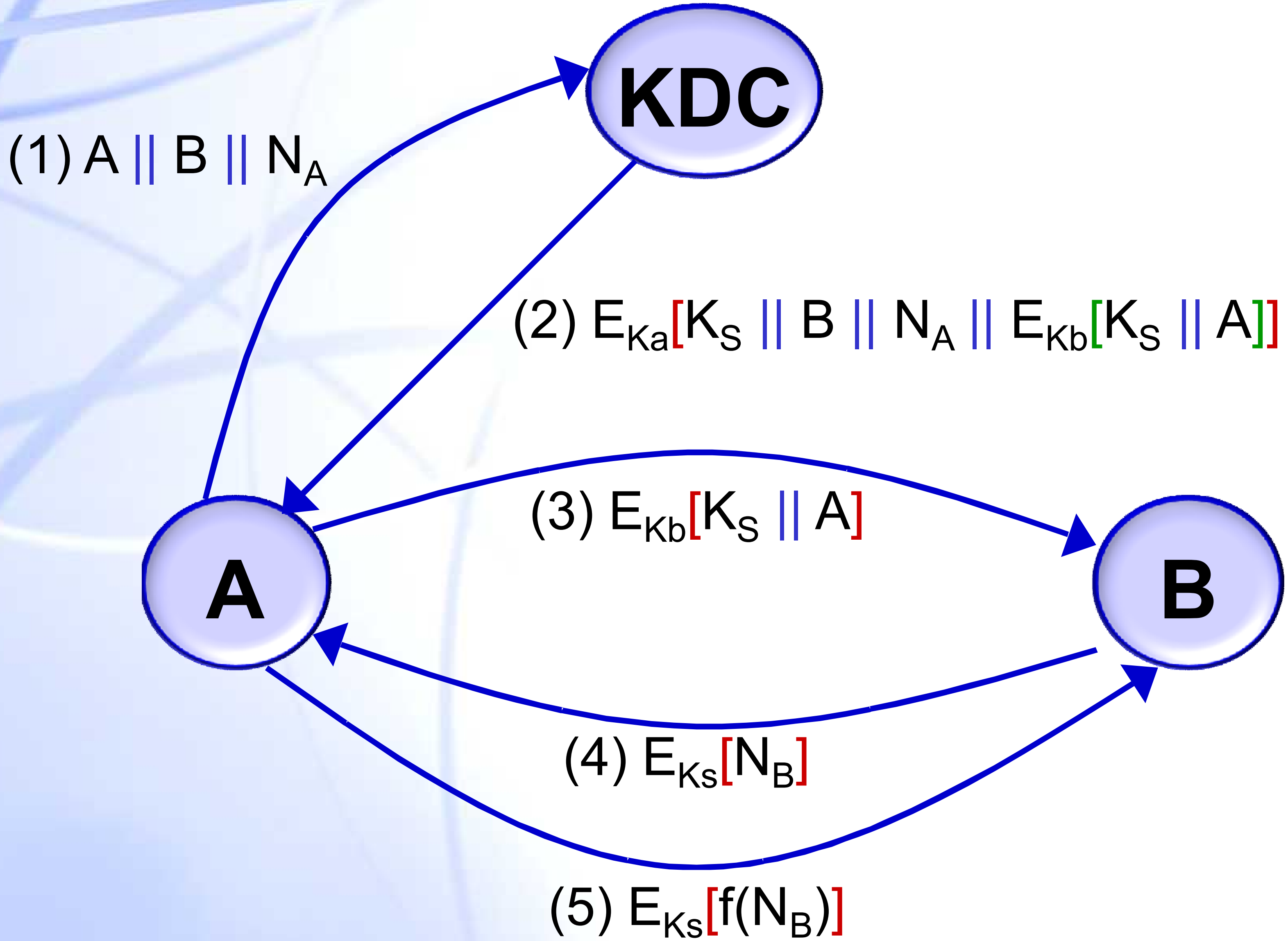


Number of required keys
(to exchange and store):

$$\boxed{\frac{N \cdot (N-1)}{2}}$$

N= 100 nodes ⇨ 5000
N=1000 nodes ⇨ 500000

NEEDHAM-SCHROEDER



CONCLUSIONS

- **Asymmetric encryption is NOT more secure than symmetric encryption**
  - To obtain a similar security degree:
    - ✓ Symmetric encryption: 128 bits keys
    - ✓ Asymmetric encryption: 1024 bits keys
  - Asymmetric encryption is significantly slower than symmetric
    - ✓ 1000 times (hardware) and 100 times (software).
- **Does not substitute symmetric encryption. Both are applied to different purposes and they are complementary**
  - Symmetric encryption is used to encrypt with a session key.
  - Asymmetric encryption
    - ✓ Allows session key exchange
    - ✓ Digital signatures

BIBLIOGRAPHY

- **Cryptography and network security. Principles and**
  Practice. Fouth edition
  Williams Stallings. Prentice Hall. 2006
  http://williamstallings.com/
- **Network security : private communication in a public world**
  C. Kaufman, R. Perlman, M. Speciner, E. Cliffs.
  Prentice Hall, 1995
- **Handbook of applied cryptography**
  Alfred J. Menezes, Paul C. van Oorschot and
  Scott A. Vanstone.2001.
  http://www.cacr.math.uwaterloo.ca/hac/
- **The Codebreakers**
  David Kahn. Scribner. 1996.
  http://david-kahn.com/