Cryptography

Hemant Ghayvat
Department of Computer Science and Media Technology
hemant.ghayvat@lnu.se

Motivation!

What do we know about the cyberattack that forced hundreds of Swedish supermarkets to close?

AFP/The Local
news@thelocal.se
@thelocalsweden
6 July 2021
08:55 CEST

Coop

Share this article

A closed Coop store in Stockholm. Photo: Ali Lorestani/TT

Swedish supermarket chain Coop was forced to shut around 800 stores after a major cyberattack which has potentially also hit more than 1,000 companies worldwide.

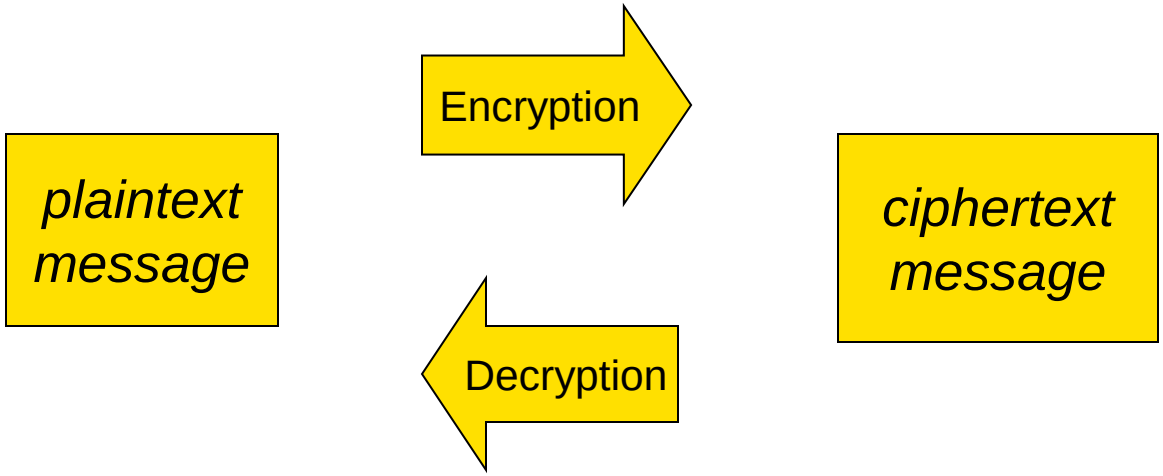
Hackers are demanding $70 million in bitcoin in exchange for data stolen in the

CIA !

Cryptography

Cryptography
Encryption
Decryption
Cipher
Key

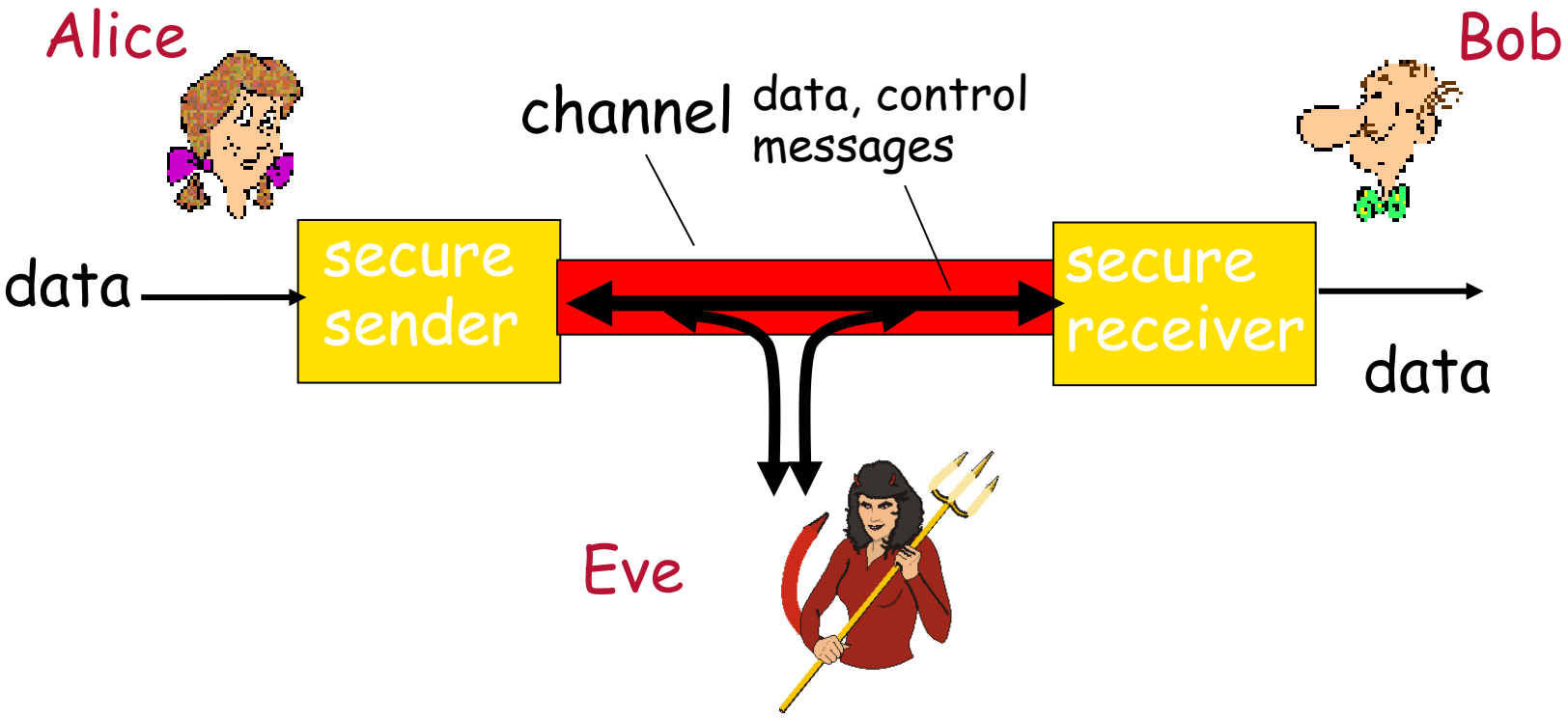
Cryptography



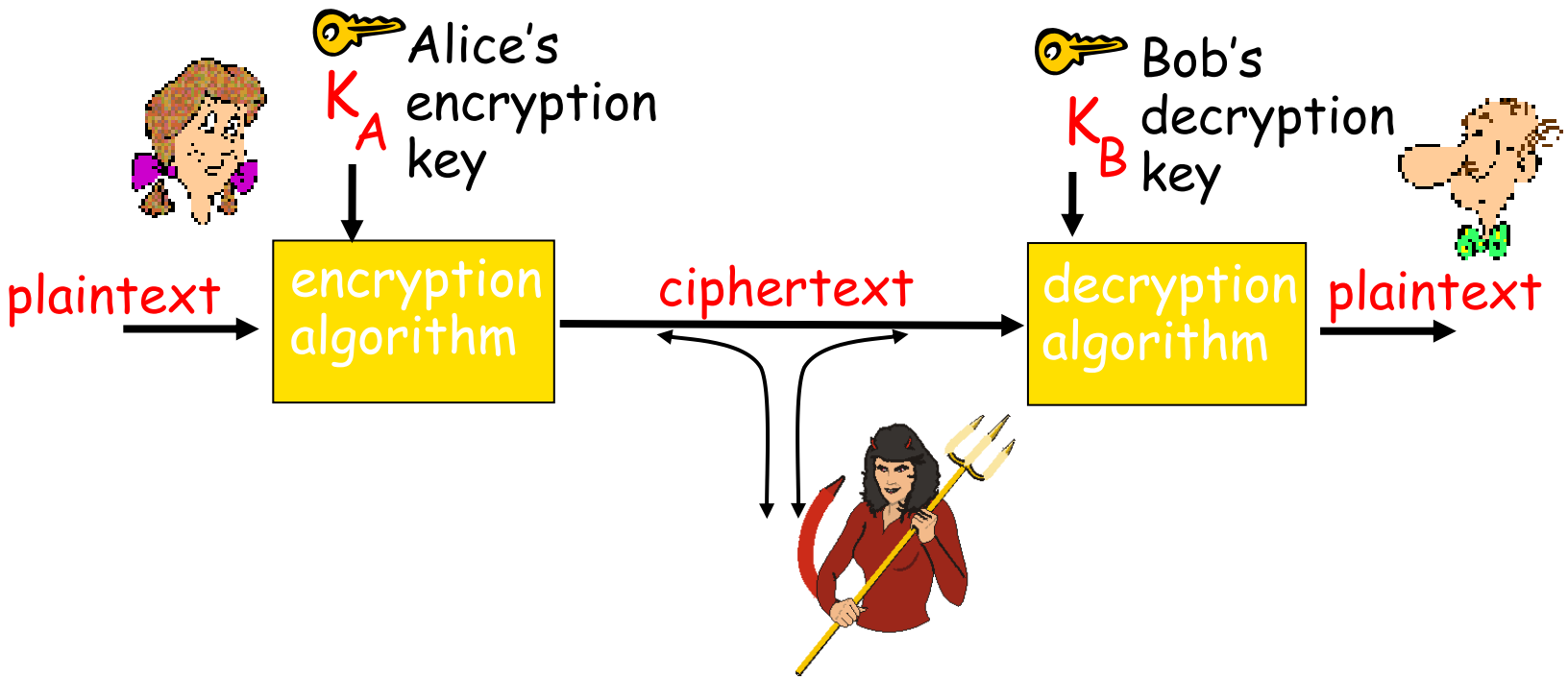
Encrypted(Information) cannot be read

Decrypted(Encrypted(Information)) can be

Friends and enemies: Alice, Bob, Trudy



The language of cryptography



symmetric key crypto: sender, receiver keys identical

Categories of Attacks

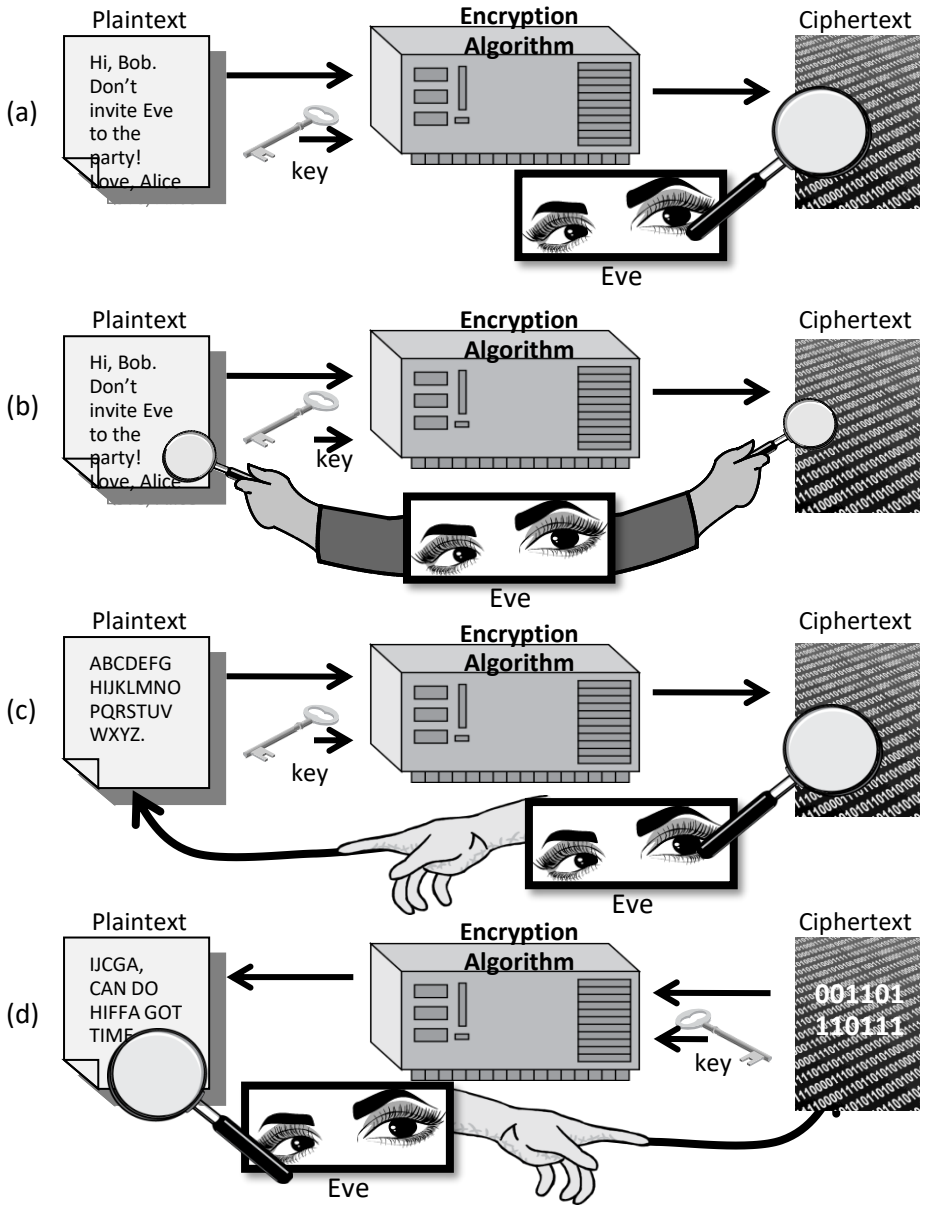
Attacker may have

a) collection of ciphertexts (ciphertext only attack)

b) collection of plaintext/ciphertext pairs (known plaintext attack)

c) collection of plaintext/ciphertext pairs for plaintexts selected by the attacker (chosen plaintext attack)

d) collection of plaintext/ciphertext pairs for ciphertexts selected by the attacker (chosen ciphertext attack)



Cryptanalysis

The process of decrypting a message without knowing the cipher or the key used to encrypt it.

Substitution and transposition ciphers are easy for modern computers to break

To protect information more sophisticated schemes are needed

What is the criteria for the secure encryption algorithm:

1. Cost of breaking is greater than the encrypted information
2. Performing the cryptanalysis would take significant amount of time, sometimes lifetime.

Brute-Force Attack

Classical Cryptography

Substitution Cipher

- Simple substitution cipher (Caesar cipher)
- Monoalphabetic Cipher
- Playfair Cipher
- Polyalphabetic Cipher

Transposition Cipher

Caesar ciphers

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

- Substitute the letters in the second row for the letters in the top row to encrypt a message

➢ Encrypt(COMPUTER) gives

FRPSXWHU

- Substitute the letters in the first row for the letters in the second row to decrypt a message

➢ Decrypt(Encrypt(COMPUTER))

= Decrypt(FRPSXWHU) = COMPUTER

Caeser Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

P(Plain text) = HELLO WORLD

K = 3 ; formula for ciphertent (C)

Encryption:-

$C = (P+K) \bmod 26$

Let's begin with H

$C_H = (7+3) \bmod 26 \Rightarrow 10 \bmod 26$

↑ weight value from above

$C_H \Rightarrow 10$ [we did't perform modulas operation as remainder would be in decimal point]

$C_H = K$

Similarely P ⇒ HELLO WORLD

↓ ↓ ↓ ↓ ↓ ↓

C ⇒ K HOOR

Decryption

$P = (C-K) \bmod 26$

$P_K = (10-3) \bmod 26 \Rightarrow 7 \bmod 26 \Rightarrow 7$

$P_K = H$

Let's take some moreel examples

Plaintext (P) = XYZ

$C_{xy} = (24+3) \bmod 26$

$= 27 \bmod 26$

$= 1 \Rightarrow B$

$C_X = (23+3) \bmod 26$

$= 26 \bmod 26 \Rightarrow 0 \Rightarrow A$

$C_Z = (25+3) \bmod 26 \Rightarrow 28 \bmod 26$

$\Rightarrow 2 \Rightarrow C$

$C_{(XYZ)} \Rightarrow ABC$

Now let's calculate plaintext (Decry

$P_A = (C-K) \bmod 26 \Rightarrow (0-3) \bmod 26$

$\Rightarrow -3 \bmod 26$ [In mod negative ⊗ not allowed]

$\Rightarrow (26-3) \bmod 26 \Rightarrow 23 \bmod 26$

$\Rightarrow 23 \Rightarrow X$

Brute Force Crypto Analysis of the Caesar Ciphers

- Brute-force cryptanalysis
- ➢ Simply try all the 25 possible keys

- Three issues with Caesar that make it vulnerable against the brute force:
  1. The encryption/decryption algorithm are known
  2. There are only 25 keys to try
  3. The language of the plaintext is known and easily recognized

Monoalphabetic Cipher

- Rather than just shifting the alphabet could shuffle (jumble) the letters arbitrarily

- Each plaintext letter maps to a different random cipher text letter hence key is 26 letters long (26! (permutation combination) Or greater than 4*1026 possible keys)

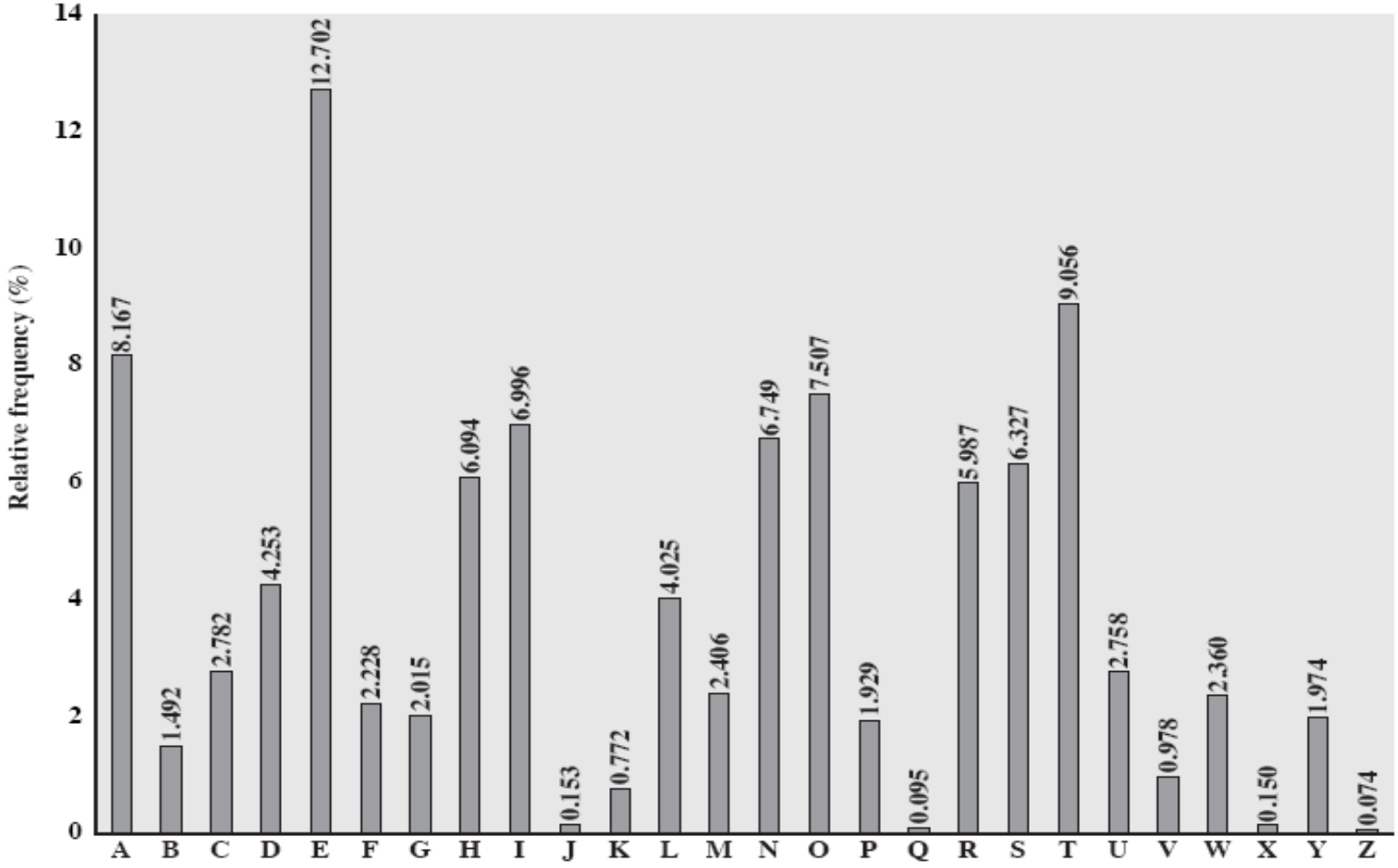
  Plain: abcdefghijklmnopqrstuvwxyz
  Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN
  Plaintext: ifwewishtoreplaceletters
  Cipher text: WIRFRWAJUHYFTSDVFSFUUFYA

Monoalphabetic Cipher Security

With so many keys, might think the system is secure

But would be **!!!WRONG!!!**

English Letter Frequencies



Polyalphabetic Cipher

- Instead of having one key (table) that is used to encrypt each block of plaintext, we use several different keys.

- The Vigenère cipher is the classical example.

Vigenere Cipher

- Idea: Uses Caesar's cipher with various shifts, in order to hide the distribution of the letters.
- A key defines the shift used in each letter in the text
- A key word is repeated as many times as required to become the same length

Vigenere Cipher

Step 1: Make a table with alphabets in the very first row and column

	A	B	C	D	E	F	...	Z
A	A	B	C	D	E	F		
B	B	C	D	E	F	G		
C	C	D	E	F	G	H		
D	D	E	F	G	H	I		
E	E	F	G	H	I	J		
F	F	G	H	I	J	H		
⋮								
Z								

Step 2: Follow RHS row to fill the table.

Example:

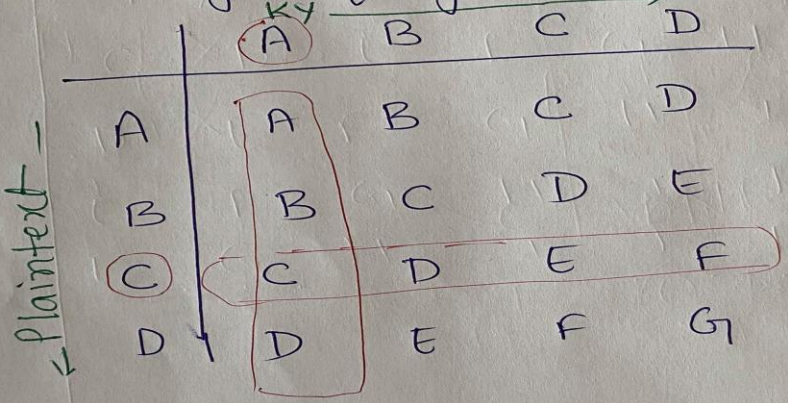
P = CAD

K = ADD

C = ?

Encryption

Step I: Make a table within the range of given alphabets (A to D)



Step II: find the plaintext row and fix it. followed fixing the column of corresponding key alphabet.

Step III: Intersaction of row (from plaintext) with column (from key)

C = C D G

Now from ciphertext (C), we have to find plaintext

C = CDG

K = ADD

P = ?

Decryption

Step I: Draw the table, now (vertical) extreme column would be key

	A	B	C	D
A	A	B	C	D
B	B	C	D	E
C	C	D	E	F
D	D	E	F	G

Key

Step II: first letter of ciphertext is C for this we need to find P. Now the corresponding key is A. The row in the key A is marked (fixed).

Step III: Now we have to find the corresponding ciphertext C in the marked row. The letter in the top most row of ciphertext alphabet is C

SO:- P = CAD

Playfair Cipher

Playfair Cipher

- Not even the large number of keys in a monoalphabetic cipher provides security
- One approach to improving security was to encrypt multiple letters
- The Playfair Cipher is an example

Playfair Key Matrix

- A 5X5 matrix of letters based on a keyword (i.e. the given plaintext is of 5 alphabets)
- Fill in letters of keyword
- Fill rest of matrix with other letters

eg. using the keyword MONARCHY

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

Encrypting and Decrypting

- plaintext encrypted two letters at a time:
  - if a pair is a repeated letter, insert a filler like 'X',
    eg. “hello" encrypts as “he lx lo“
  - if both letters fall in the same row, replace each with letter to right (wrapping back to start from end), eg. “ar" encrypts as "RM"
  - if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom),
    eg. “mu" encrypts to "CM"
  - otherwise each letter is replaced by the one in its row in the column of the other letter of the pair, eg. “hs" encrypts to "BP", and “ea" to "IM" or "JM"

Playfair Cipher

⇒ P= WORLD , K= SECURE

C= ?

It is 5×5 matrix (as the P is 5)

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

→ Fill 5 keys alphabets into first row, but do not repeat any alphabet (i.e. wrote E once)

← Now in the rest of the boxes fill remaining alphabets (other than SECUR)

✡ most of books consider I/J together

⇒ Now you have to make pair of alphabets in the given P so

WORLD ?

WO RL DX (Usually)

⇒ Encryption

P= WO RL DX

P_1 P_2 P_3

K= SECURE

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

C=

Rule 1:

P_1 (WO) are coming in the same column, then the cipher would be the letter below. So below W is (E). Below O is (W). C_1 = EW

Rule 2:

P_2 (RL) are coming in different row and column, then the cipher would be calculated by forming a rectangle covering the R and L.

The letter on the corner and opposite would be ~~are~~ answer. C_2 = UM

U	R
F	G
L	M

Playfair Cipher

⇒ P = WORLD , K = SECURE

C = ?

It is 5×5 matrix (as the P is 5)

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

→ Fill 5 keys alphabets into first row, but do not repeat any alphabet (i.e. wrote E once)

← Now in the rest of the boxes fill remaining alphabets (other than SECUR)

✡ most of books consider I/J together

⇒ Now you have to make pair of alphabets in the given P

So

WORLD ?

WO RL DX (usually)

Rule 1:

P_3 (DX) are in same column

So C_3 = KC

C = EWVMKC

Rule 3 (which we donot need in the current example)

~~let~~ let's we have plaintext P_3 (OP), then the cipher would be the letter next to plaintext letter C_3(PQ). [whenever Plaintext comes in same row]

Now if P_3 (BG), C_3 = ? DA

Playfair Cipher

⇒ P = WORLD , K = SECURE

C = ?

It is 5×5 matrix (as the P is 5)

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

→ Fill 5 keys alphabets into first row, but do not repeat any alphabet (i.e. wrote E once)

← Now in the rest of the boxes fill remaining alphabets (other than SECUR)

✡ most of books consider I/J together

⇒ Now you have to make pair of alphabets in the given P so

WORLD ?

WO RL DX (usually)

Decryption:

Now we have to find the P for C = EW UM KC

C_1 C_2 C_3

Again form the pair

Rule 1

C_1 = EW

EW are coming in same column so in decryption we will find by seeing the letter above the plaintext (in encryption we were seeing letter below)

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

P_1 = WO

Rule 2

C_2 = UM

P_2 = RL

U	R
F	G
L	M

Rule 1

C_3 = KC ⇒ P_3 = DX — Discared

P = WO RL DX → Discared

Security of the Playfair Cipher

- Security much improved over monoalphabetic

since have 26 x 26 = 676 digrams

- Would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic) and correspondingly more ciphertext

One-Time Pads (Vernam Cipher)

- Extended from Vigenere cipher
- There is one type of substitution cipher that is absolutely unbreakable.
- The message is represented as a binary string (a sequence of 0's and 1's using a coding mechanism such as ASCII coding.
- The key is a truly random sequence of 0's and 1's of the same length as the message.
- The encryption is done by adding the key to the message modulo 2, bit by bit. This process is often called *exclusive or*, and is denoted by *XOR*. The symbol $\oplus$ is used
- Length of the key should be equal to plaintext

VERNAM CIPHER

Example:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

R	S	T	U	V	W	X	Y	Z
17	18	19	20	21	22	23	24	25

Plaintext → D A N D A P A N I , Key = E R I S H P A U L

Encryption: Draw a table with the weight values of letters

$C_t = P_t + Key$

C_t = H R V V H E A H T

P_t	3	0	13	3	0	15	0	13	8
Key	4	17	8	18	7	15	0	20	11
C_t	7	17	21	21	7	4	0	7	19

↓(If C_t > 25)

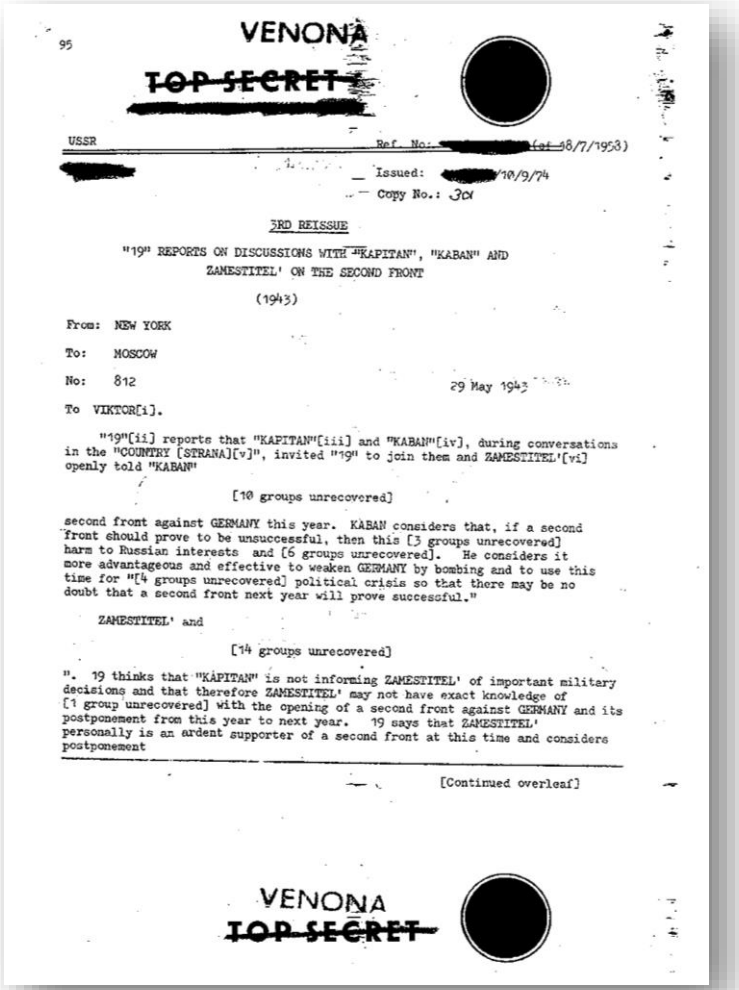
Decryption:-

$P_t = C_t - Key$

C_t	7	17	21	21	7	4	0	7	19
Key	4	17	8	18	7	15	0	20	11
	3	0	13	3	0	-11	0	-13	8
	3	0	13	3	0	15	0	13	8
	D	A	N	D	A	P	A	N	I

Weaknesses of the One-Time Pad

- In spite of their perfect security, one-time pads have some weaknesses
- The key has to be as long as the plaintext
- Keys can never be reused
  - Repeated use of one-time pads allowed the U.S. to break some of the communications of Soviet spies during the Cold War.



95

VENONA

~~TOP SECRET~~ [redacted]

USSR

Ref. No: [redacted] (of 18/7/1958)

[redacted] Issued: [redacted] 10/9/74

Copy No.: 301

3RD REISSUE

"19" REPORTS ON DISCUSSIONS WITH "KAPITAN", "KABAN" AND ZAMESTITEL' ON THE SECOND FRONT

(1943)

From: NEW YORK

To: MOSCOW

No: 812

29 May 1943

To VIKTOR[i].

"19"[ii] reports that "KAPITAN"[iii] and "KABAN"[iv], during conversations in the "COUNTRY [STRANA][v]", invited "19" to join them and ZAMESTITEL'[vi] openly told "KABAN"

[10 groups unrecovered]

second front against GERMANY this year. KABAN considers that, if a second front should prove to be unsuccessful, then this [3 groups unrecovered] harm to Russian interests and [6 groups unrecovered]. He considers it more advantageous and effective to weaken GERMANY by bombing and to use this time for "[4 groups unrecovered] political crisis so that there may be no doubt that a second front next year will prove successful."

ZAMESTITEL' and

[14 groups unrecovered]

". 19 thinks that "KAPITAN" is not informing ZAMESTITEL' of important military decisions and that therefore ZAMESTITEL' may not have exact knowledge of [1 group unrecovered] with the opening of a second front against GERMANY and its postponement from this year to next year. 19 says that ZAMESTITEL' personally is an ardent supporter of a second front at this time and considers postponement

[Continued overleaf]

VENONA

~~TOP SECRET~~

Transposition ciphers

- An alternative to substitution ciphers
- Instead of changing the coding of the characters (blocks) in the plaintext, we rearrange the text.
- The effect is that the cipher text and the plaintext contains the same symbols.
- Algorithm

➢ Divide to plaintext into blocks

➢ Decide on a permutation order

➢ Rearrange the blocks according to this

Transposition ciphers

In the transposition technique the positions of letters/numbers/symbols in plain text is changed with one another.

1	2	3	4	5	6
M	E	E	T	M	E
A	F	T	E	R	P
A	R	T	Y		

4	2	1	6	3	5
T	E	M	E	E	M
E	F	A	P	T	R
Y	R	A		T	

Problems with classical ciphers

- Neither substitution nor transposition ciphers are secure enough today
- They also often have problems with complex keys that are hard to remember
- Solution?
- Hybrid approach by combining both methods

Stream and Block Ciphers

- Both uses symmetric encryption key
- Stream Cipher: It encrypts a digital data stream one bit or 1 byte at a time
- Block Ciphers: In this a block of plain text is treated as a whole and used to produce the ciphertext of equcl length, Typically a block size of 64 or 128 bits.

Block Ciphers

Block Cipher

- Plaintext and ciphertext consists of fixed sized blocks
- Ciphertext obtained from plaintext by iterating a round function
- Input to round function consists of key and the output of previous round
- Usually implementation friendly. Gives a high throughput.

Feistel Cipher

- Feistel cipher refers to splitting the plaintext into two equal parts
- Split plaintext block into left and right halves: Plaintext = (L_0,R_0)
- These two halves of the data pass through n rounds of processing and then combine to produce the ciphertext block
- For each round i=1,2,...,n, compute

  $L_i = R_{i-1}$

  $R_i = L_{i-1} \oplus F(R_{i-1},K_i)$

  where F is round function and K_i is subkey (*refer next slide for it*)
- Ciphertext = (L_n,R_n)

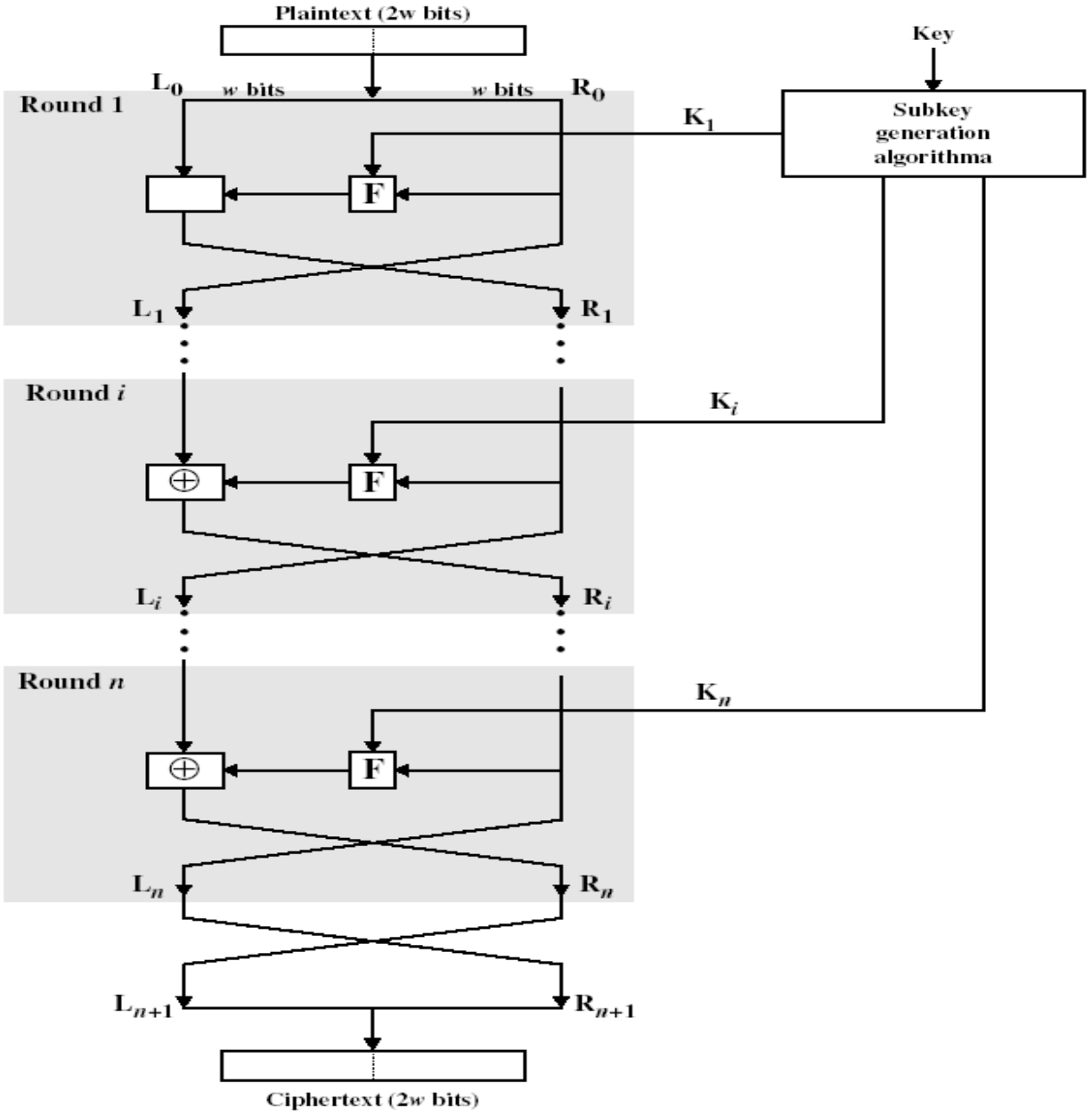
Feistel Cipher: Sub Key

- On the right half we apply a function and in the function, we use a subkey generated from the master key (main key)
- A substitution is performed on the left half of the data. This is done by applying a round function to the right half of the data followed by the XOR of the output of that function and the left half of the data.
- That’s count the first round.
- All rounds have the same structure
- All conventional block encryption algorithms including data encryption standard (DES) are based on Feistel Cipher Structure.

Feistel Cipher

- Decryption: Ciphertext = (L_n,R_n)
- For each round i=n,n–1,…,1, compute
  $R_{i-1} = L_i$
  $L_{i-1} = R_i \oplus F(R_{i-1},K_i)$
  where F is round function and K_i is subkey
- Plaintext = (L_0,R_0)
- Formula “works” for any function F
- But only secure for certain functions F

Classical Feistel Network



Design Features of Feistel Network

- **Block Size:** (larger block means greater security).
- **Key Size**:56-128 bits.
- **Number of Rounds**: a single round offers inadequate security, a typical size is 16 rounds.
- **Sub-key Generation Algorithms**: greater complexity should lead to a greater difficulty of cryptanalysis.
- **Round function:** Again, greater complexity generally means greater resistance to cryptanalysis.

Block Ciphers in Practice

Data Encryption Standard (DES)

- Developed by IBM and adopted by NIST in 1977
- 64-bit blocks and 56-bit keys
- Small key space makes exhaustive search attack feasible since late 90s

Triple DES (3DES)

- Nested application of DES with three different keys KA, KB, and KC
- Effective key length is 168 bits, making exhaustive search attacks unfeasible
- $C = E_{KC}(D_{KB}(E_{KA}(P)))$; $P = D_{KA}(E_{KB}(D_{KC}(C)))$
- Equivalent to DES when KA=KB=KC (backward compatible)

Advanced Encryption Standard (AES)

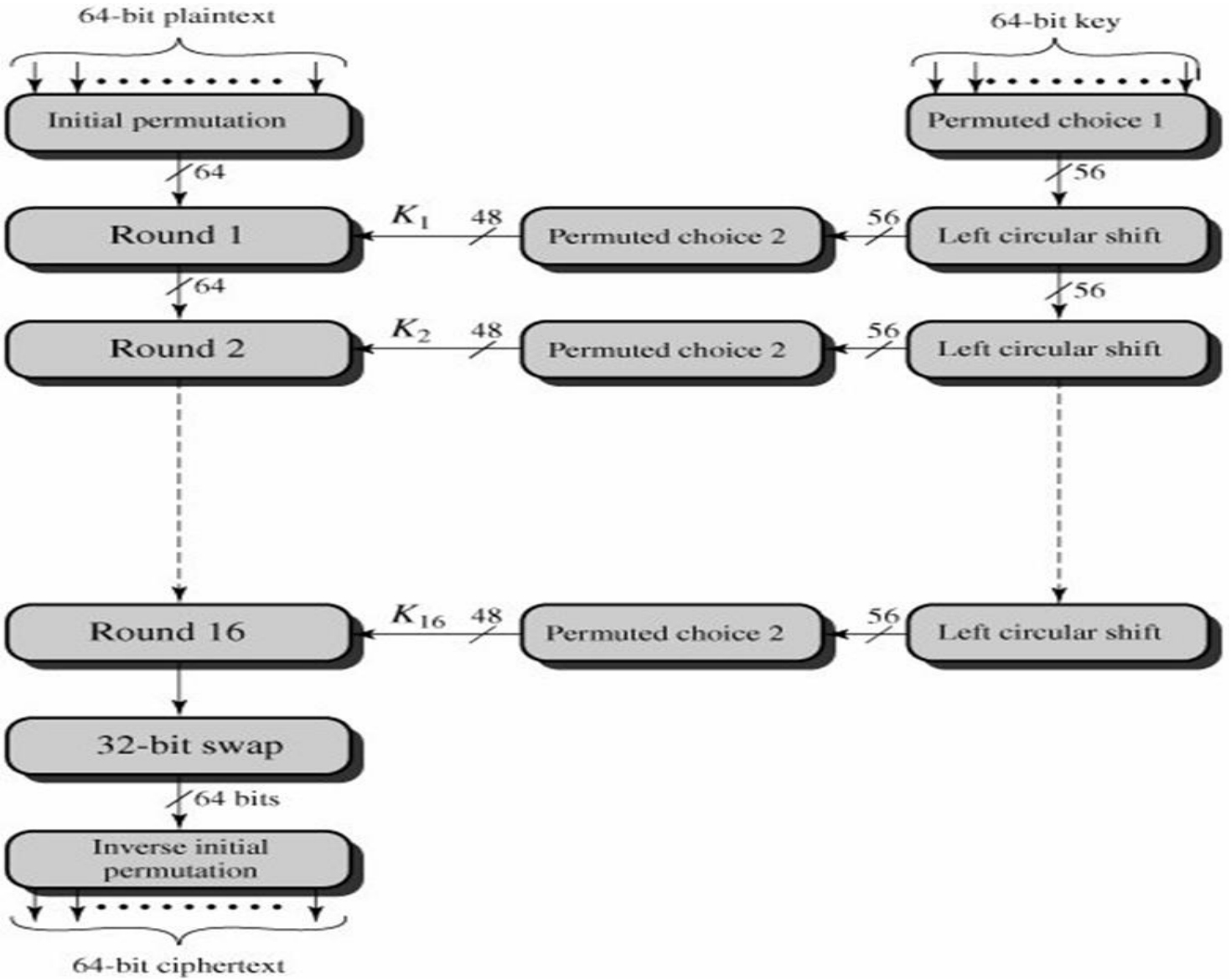
- Selected by NIST in 2001 through open international competition and public discussion
- 128-bit blocks and several possible key lengths: 128, 192 and 256 bits
- Exhaustive search attack not currently possible
- AES-256 is the symmetric encryption algorithm of choice

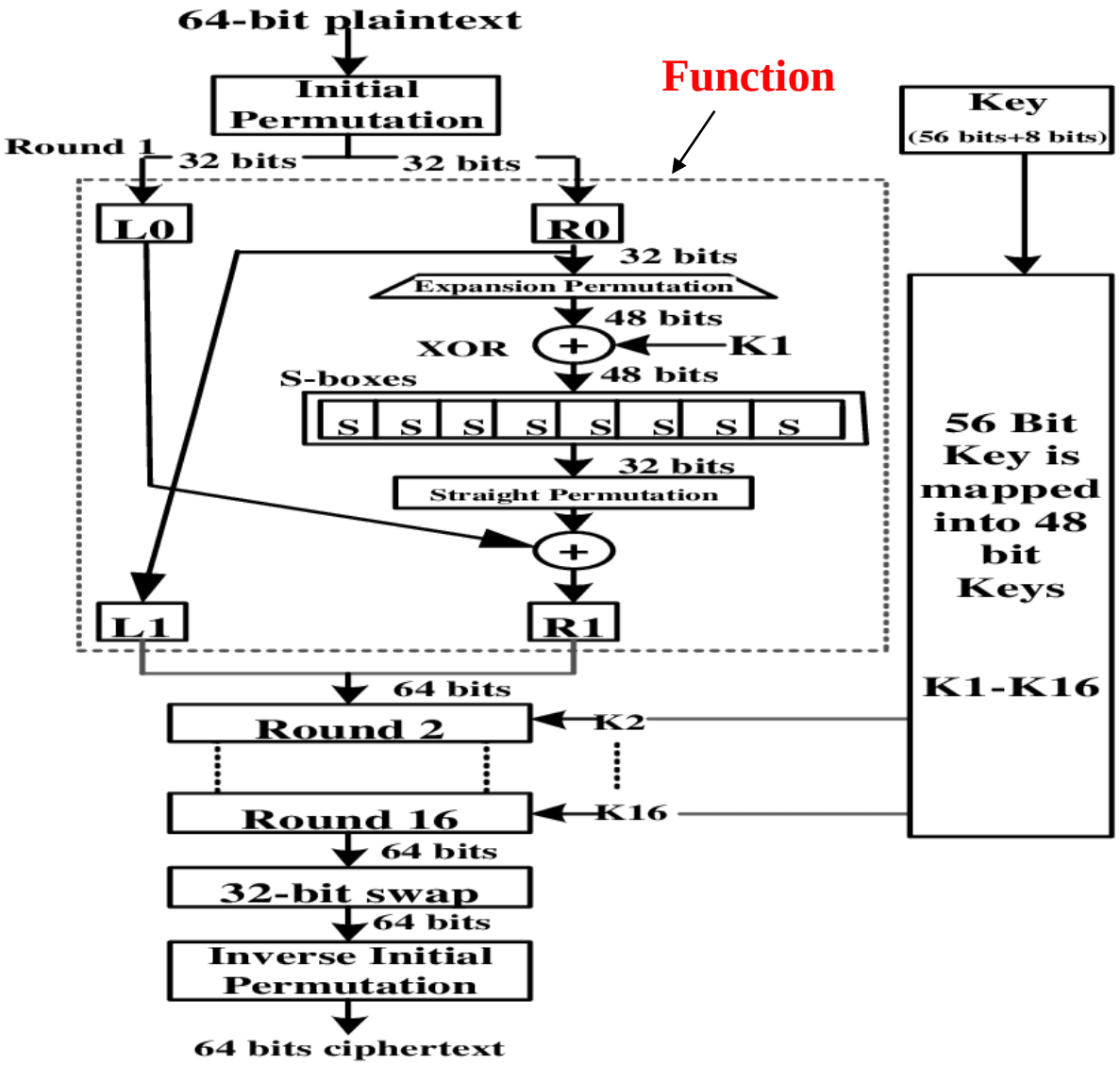
Data Encryption Standard (DES)

- Block Cipher
- Symmetric cipher (same Keys for the encryption and decryption)
- 64 bit plaintext block
- 16 fiestel round

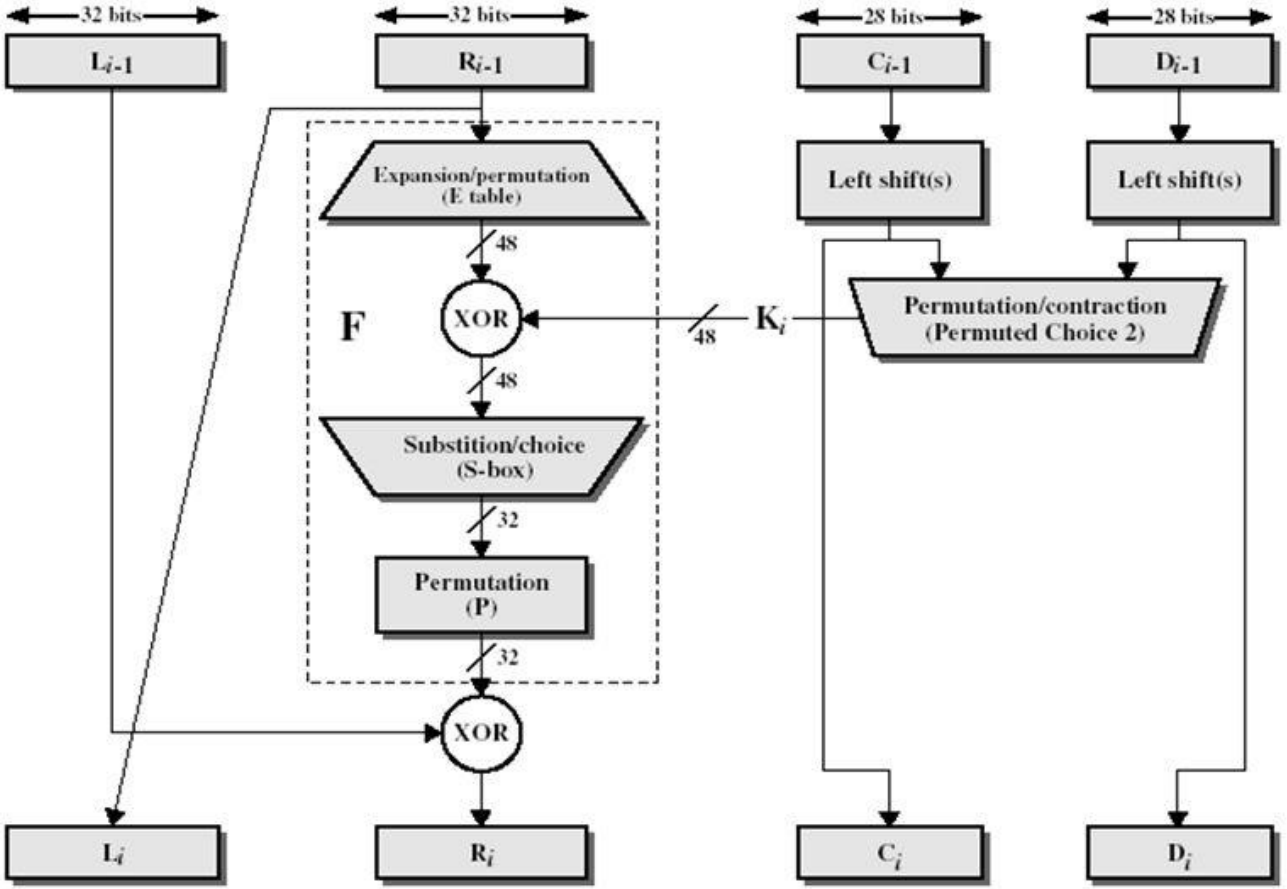
- Steps in DES:

I. Initial Permutation
II. 16 Feistel rounds
III. Swapping or left right swap
IV. Final permutation or inverse initial permutation


64-bit plaintext
64-bit key
Initial permutation
Permuted choice 1
64
56
Round 1
K_1
48
Permuted choice 2
56
Left circular shift
64
56
Round 2
K_2
48
Permuted choice 2
56
Left circular shift
Round 16
K_{16}
48
Permuted choice 2
56
Left circular shift
32-bit swap
64 bits
Inverse initial permutation
64-bit ciphertext

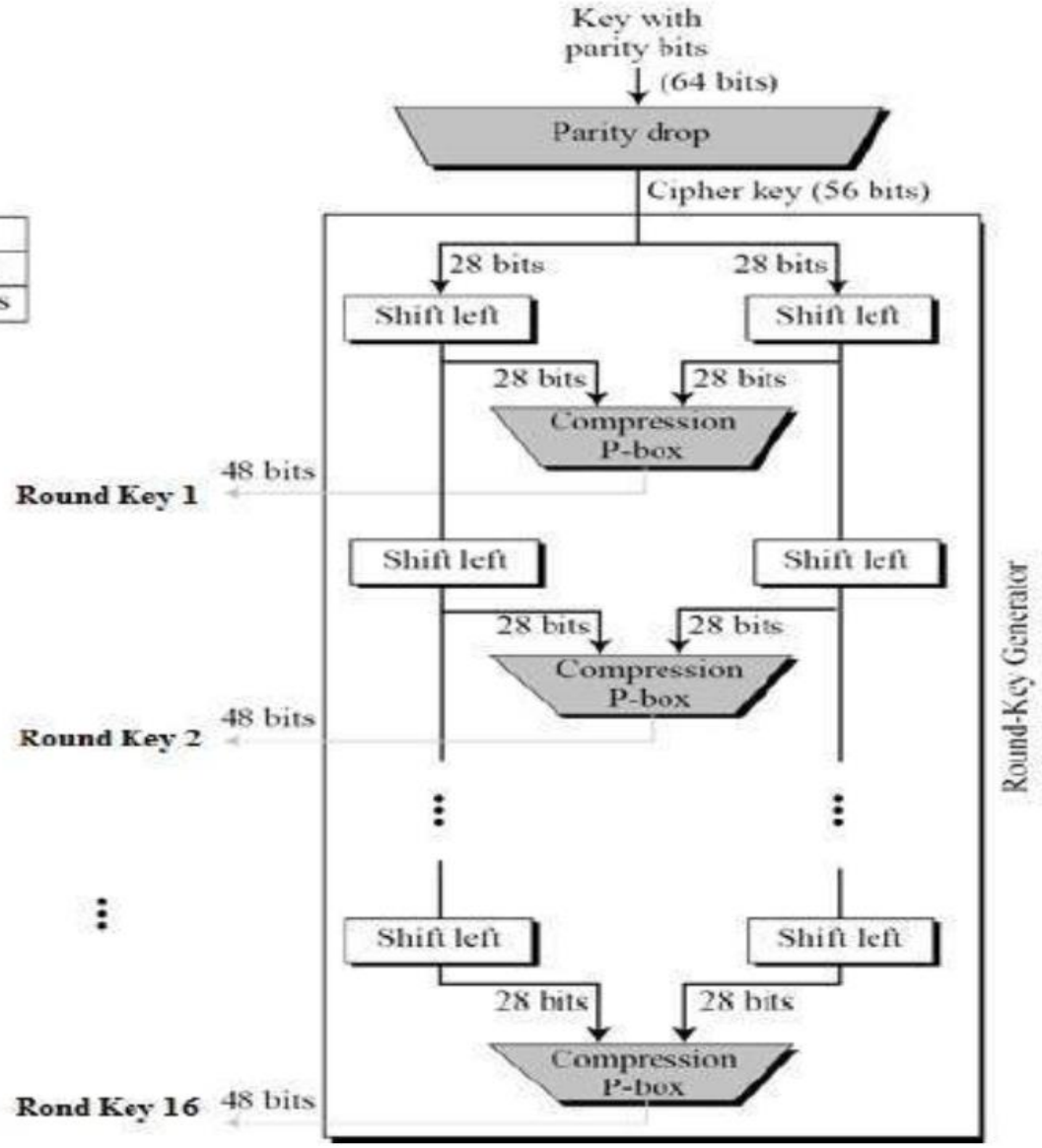

64-bit plaintext
Initial Permutation
Round 1
32 bits
32 bits
L0
R0
Function
Key
(56 bits+8 bits)
32 bits
Expansion Permutation
48 bits
XOR
K1
S-boxes
48 bits
S S S S S S S S
32 bits
Straight Permutation
L1
R1
56 Bit Key is mapped into 48 bit Keys
K1-K16
64 bits
Round 2
K2
Round 16
K16
64 bits
32-bit swap
64 bits
Inverse Initial Permutation
64 bits ciphertext

Single Iteration of DES Algorithm



Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits



DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- **Avalanche effect** − A small change in plaintext results in the very great change in the ciphertext.
- **Completeness** − Each bit of ciphertext depends on many bits of plaintext.

- Problem with DES

➢ Broken in 1998 by Electronic Frontier Foundation

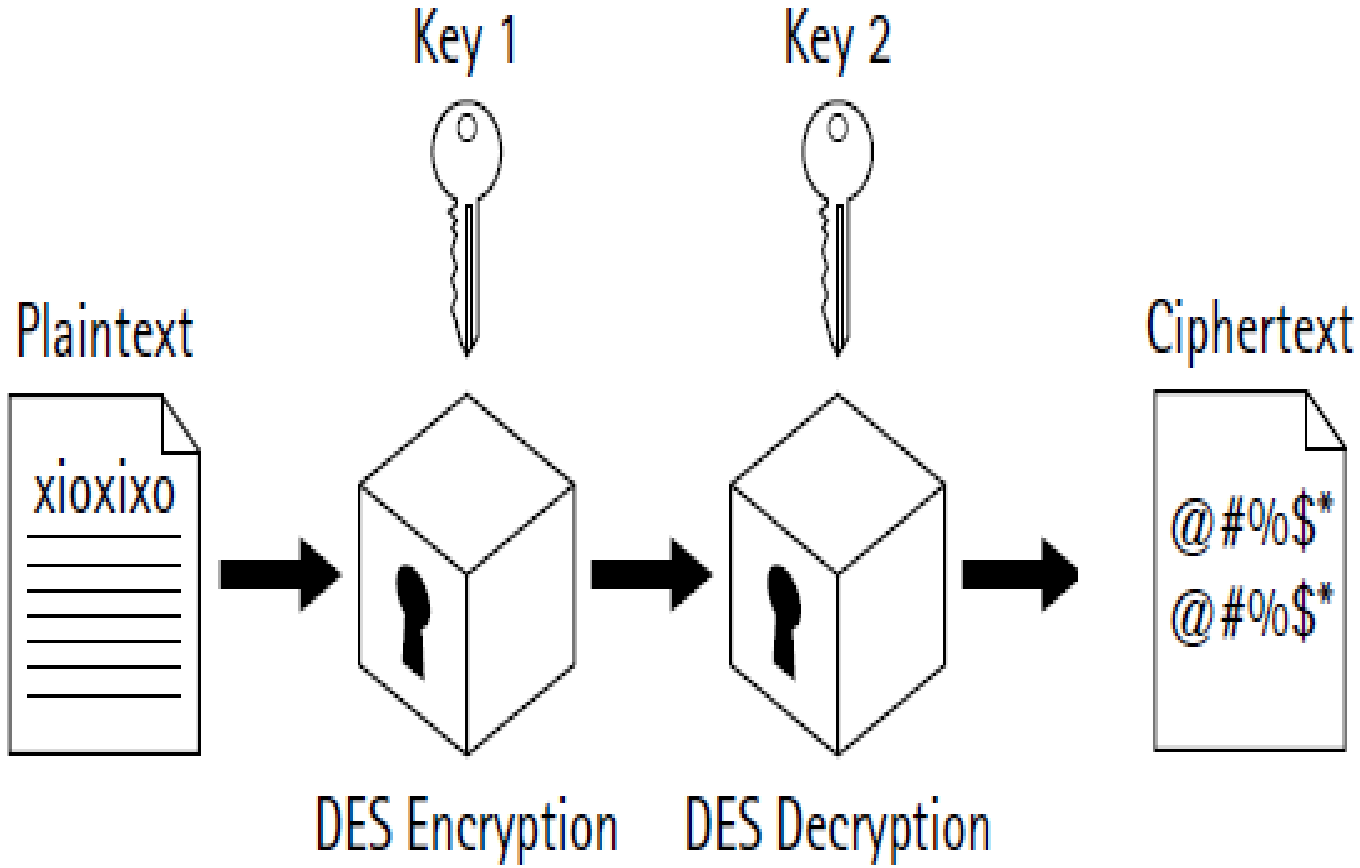
➢ Used special purpose machine - $250,000 [a]Took less than three days

Double DES

- DES uses a 56-bit key, this raised concerns about brute force attacks.
- Double uses two keys, K1 and K2
- Perform DES on the plaintext using K1 to get encrypt text.
- Again, perform DES on the encrypt text using K2.
- The final output is the encryption of the encrypted text.
- his leads to a 2x56=112 bit key, so it is more secure than DES. Is it?
- Double DES has a 112-bit key, and ciphers blocks of 64 bits.

$$p \rightarrow E(k_1, \quad p) \rightarrow E(k_2, \quad E(k_1, \quad p)) = C$$

Double DES


Key 1
Key 2
Plaintext
xioxixo
Ciphertext
@#%$*
@#%$*
DES Encryption
DES Decryption

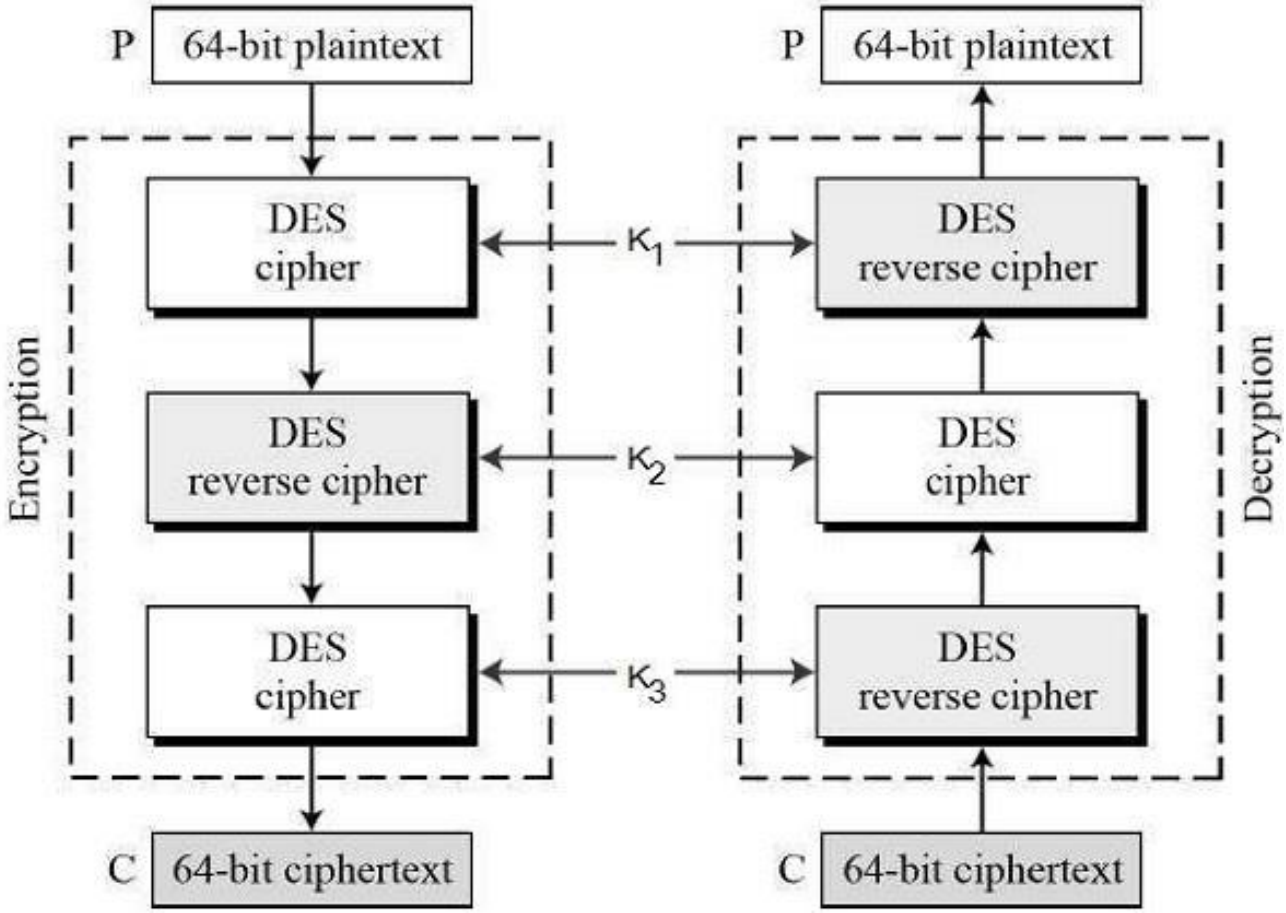
Meet-in-the-Middle Attack (MIM Attack)

- To improve the security of a block cipher, one might get the (naive) idea to simply use two independent keys to encrypt the data twice.
- In fact, an exhaustive search of all possible combinations of keys would take 2^{2n} attempts (if each key K1, K2 is n bits long), compared to the 2^{n} attempts required for searching a single key.
- The attacker can first compute E_{K1}(P) for all possible keys K1 and store the results in memory (in a lookup table).
- Afterwards he can decrypt the ciphertext by computing D_{K2}(C) for each K2.
- Any matches between these two resulting sets are likely to reveal the correct keys. (To speed up the comparison, the E_{K1}(P) set is stored in an in memory lookup table, then each D_{K2}(C) can be matched against the values in the lookup table to find the candidate keys.)
- Once the matches are discovered, they can be verified with a second testset of Plaintext and Ciphertext.

Triple DES

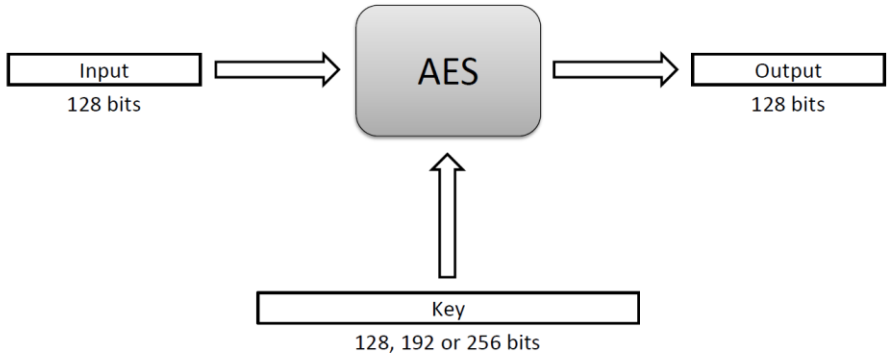
- 3DES was developed in 1999 by IBM – by a team led by Walter Tuchman. 3DES prevents a meet-in-the-middle attack. 3DES has a 168-bit key and ciphers blocks of 64 bits
- The plain text block is first encrypted with k1, then encrypted with k2 and finally with the k3
- All three keys would be different from each other
- Its three times slower than DES

Triple DES


P
64-bit plaintext
DES
cipher
DES
reverse cipher
DES
cipher
C
64-bit ciphertext
Encryption
K1
K2
K3
P
64-bit plaintext
DES
reverse cipher
DES
cipher
DES
reverse cipher
C
64-bit ciphertext
Decryption

The Advanced Encryption Standard (AES)

- clear a replacement for DES was needed
- ➢ have theoretical attacks that can break it
- ➢ have demonstrated exhaustive key search attacks
- can use Triple-DES – but slow, has small blocks
- US NIST issued call for ciphers in 1997
- 15 candidates accepted in Jun 98
- 5 were shortlisted in Aug-99
- Rijndael was selected as the AES in Oct-2000 Nov-2001



The AES Cipher - Rijndael

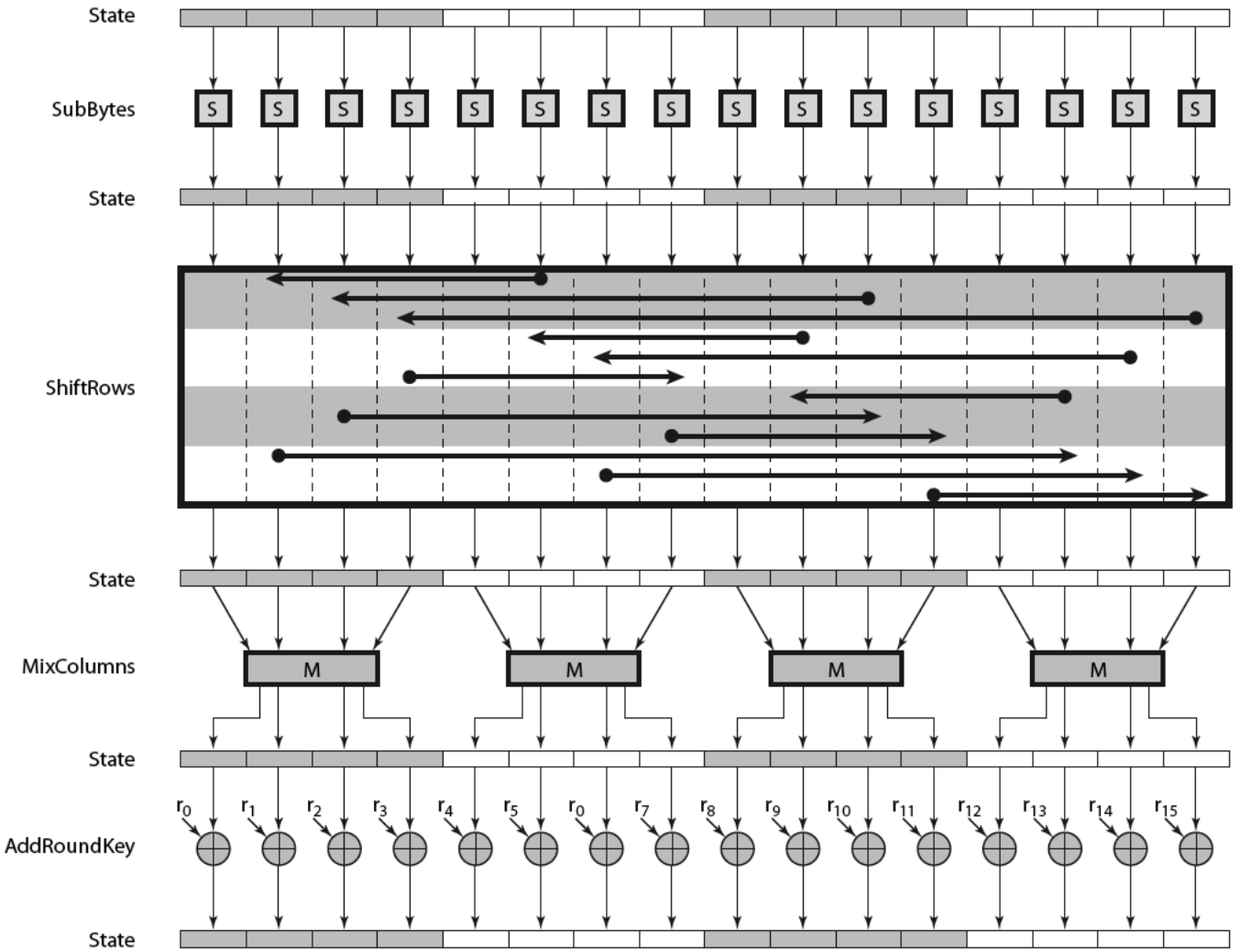
- has 128/192/256 bit keys, 128 bit data
- an **iterative** rather than **Feistel** cipher
  - processes data as block of 4 columns of 4 bytes
  - operates on entire data block in every round
- designed to have:
  - resistance against known attacks
  - speed and code compactness on many CPUs
  - design simplicity

AES Rounds

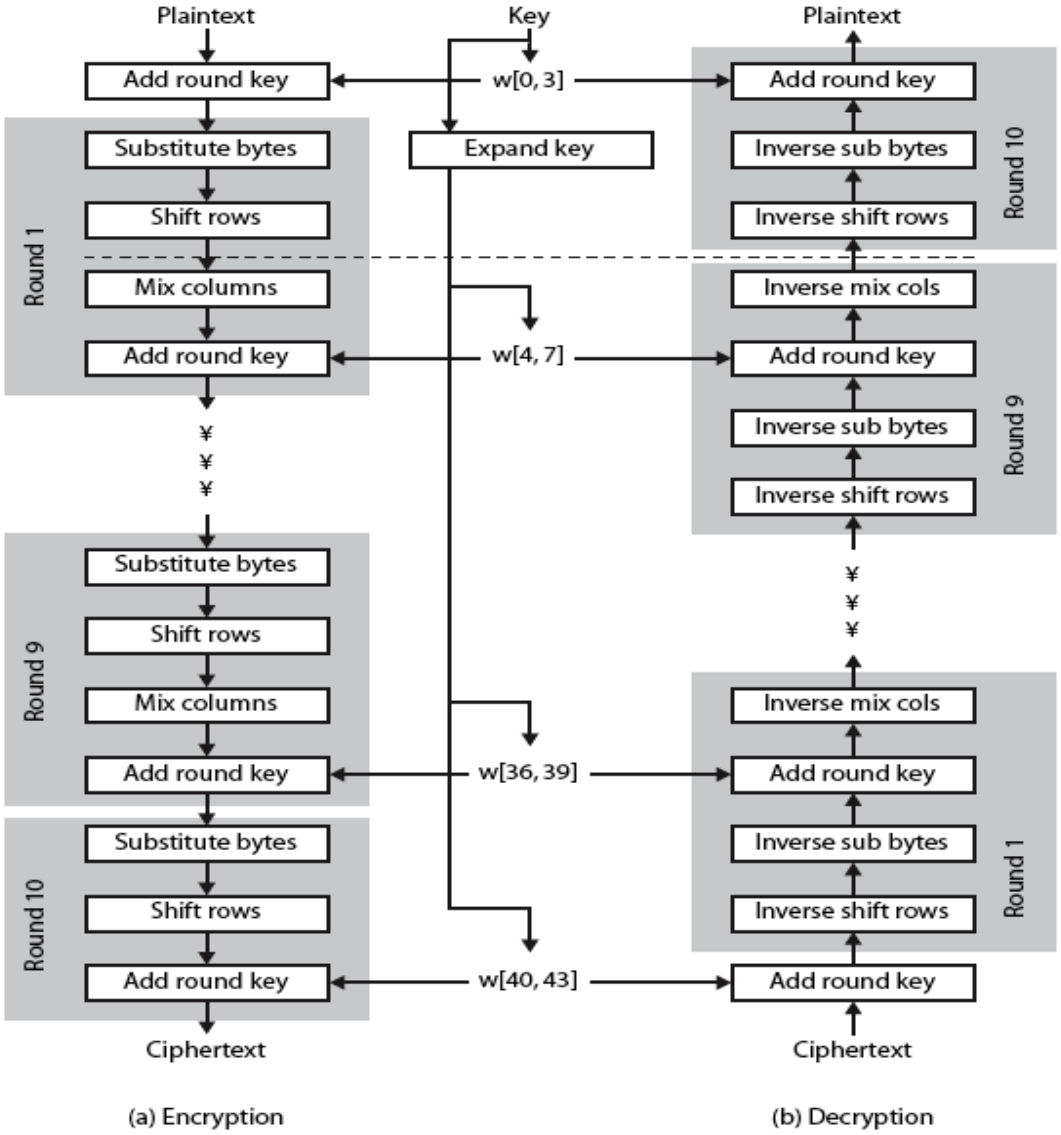
Each round is built from four basic steps:

1. SubBytes step: an S-box substitution step
2. ShiftRows step: a permutation step
3. MixColumns step: a matrix multiplication step
4. AddRoundKey step: an XOR step with a round key derived from the 128-bit encryption key

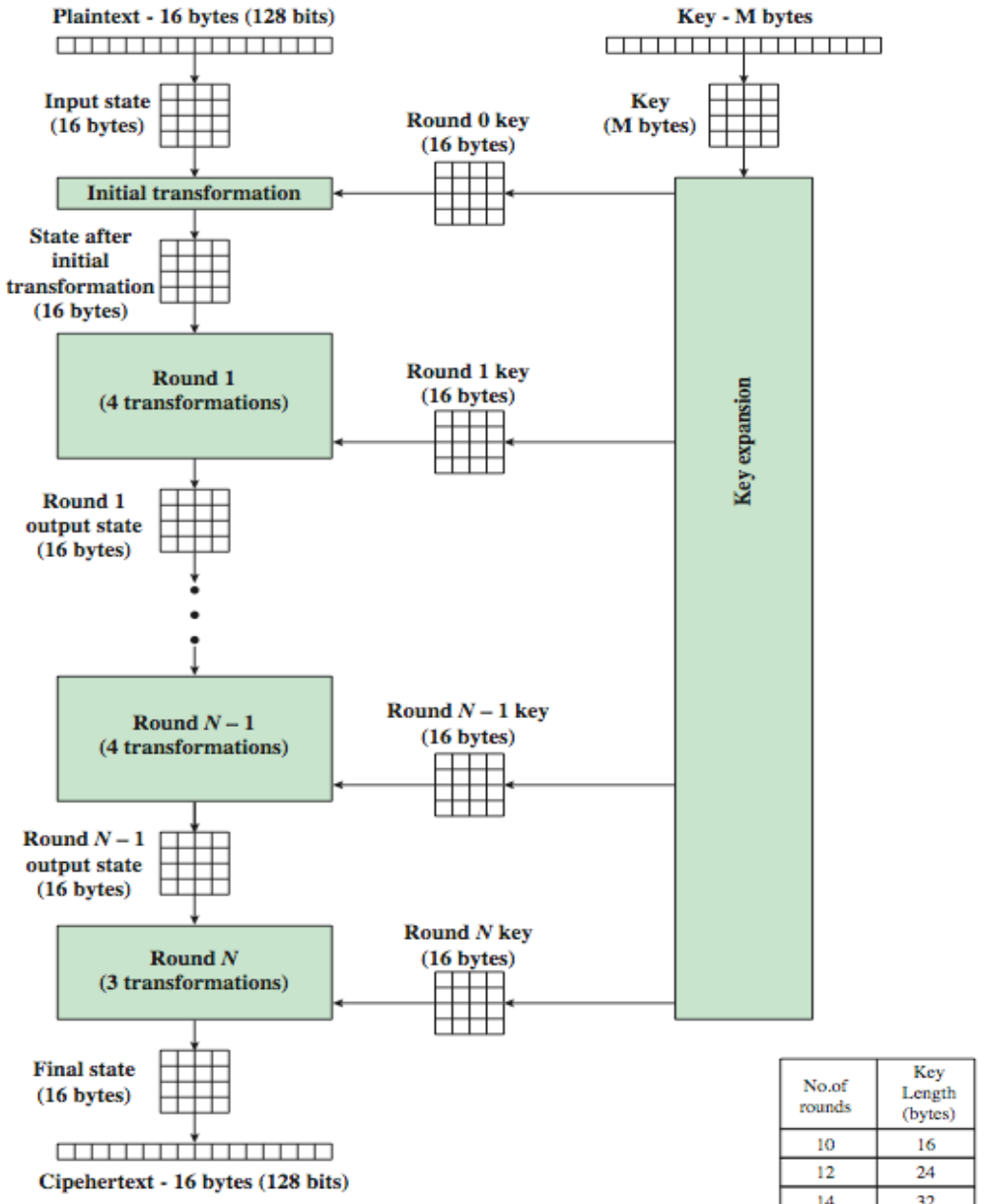
AES Round


State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
r0 r1 r2 r3 r4 r5 r0 r7 r8 r9 r10 r11 r12 r13 r14 r15
State

AES Structure

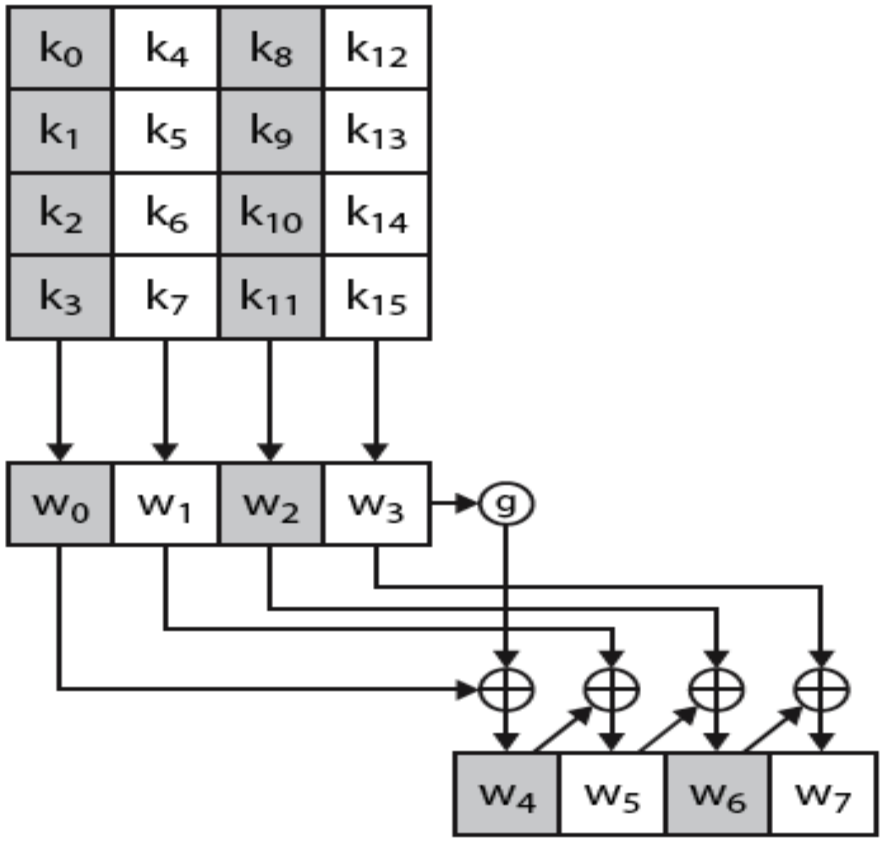


AES Encryption Process



No.of rounds	Key Length (bytes)
10	16
12	24
14	32

AES Key Expansion



Comparison table different symmetric encryption algorithms

Symmetric Key Algorithm	Structure	Key Size (bits)	No of Rounds	Block Size (bits)	Security	Speed
DES	Feistel	56	16	64	Already Broken	Slow
3 DES	Feistel	112, 168	48	64	Adequate	Very Slow
AES	Substitution/ Transposition	128, 192, 256	10, 12, 14	128	Excellent	Fast
Blowfish	Feistel	32-448	16	64	Excellent	Fast

How to use a block cipher?

- Block ciphers encrypt fixed-size blocks
  - e.g. DES encrypts 64-bit blocks
- We need some way to encrypt a message of arbitrary length
  - e.g. a message of 1000 bytes
- NIST defines several ways to do it
  - called **modes of operation**

Modes of Operation

- Block ciphers encrypt fixed size blocks
  - eg. DES encrypts 64-bit blocks, with 56-bit key
- Need way to use in practise, given usually have arbitrary amount of information to encrypt
  - Partition message into separate block for ciphering
- A **mode of operation** describes the process of encrypting each of these blocks **under a single key**

Some modes may use randomized addition input value

Five Modes of Operation

- Electronic codebook mode (ECB)
- Cipher block chaining mode (CBC) – most popular
- Output feedback mode (OFB)
- Cipher feedback mode (CFB)
- Counter mode (CTR)

Electronic Code Book (ECB)

The plaintext is broken into blocks, P_1, P_2, P_3, ...

Each block is encrypted independently:

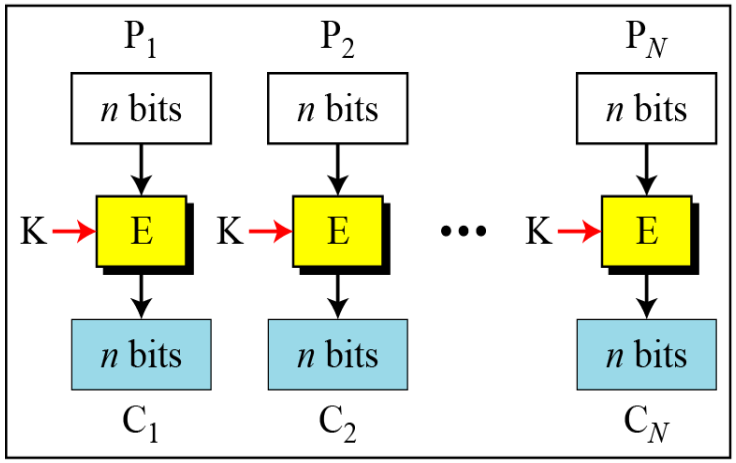
$$C_i = E_K(P_i)$$

For a given key, this mode behaves like we have a gigantic codebook, in which each plaintext block has an entry, hence the name Electronic Code Book

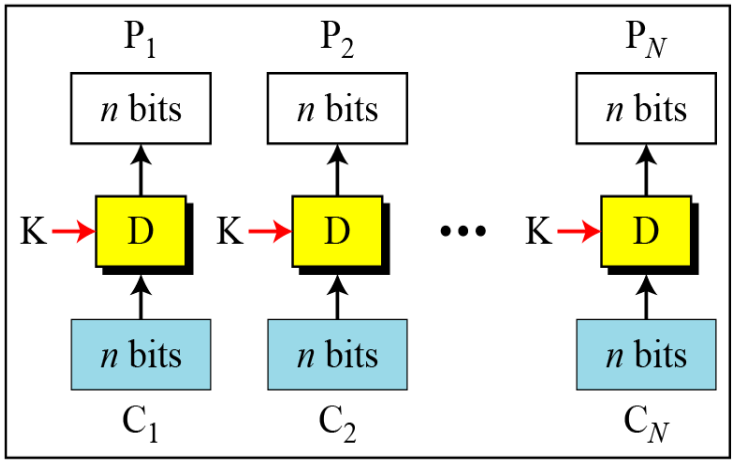
ECB Scheme

Encryption: $C_i = E_K (P_i)$ Decryption: $P_i = D_K (C_i)$

E: Encryption D: Decryption
P_i: Plaintext block i C_i: Ciphertext block i
K: Secret key



Encryption



Decryption

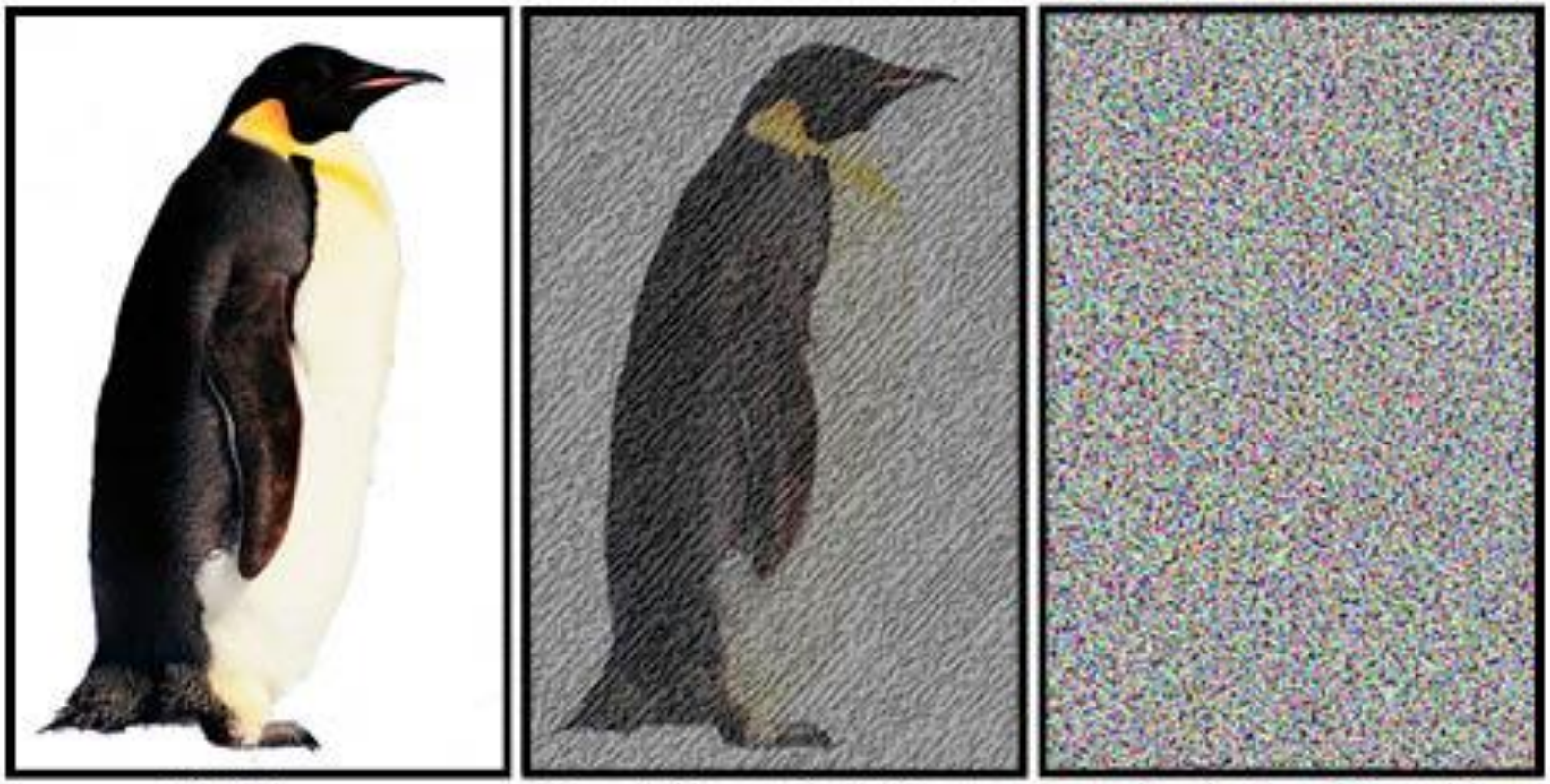
Remarks on ECB

- Strength: it's simple.

- Weakness:
  - Repetitive information contained in the plaintext may show in the ciphertext, if aligned with blocks.
  - If the same message (e.g., an SSN) is encrypted (with the same key) and sent twice, their ciphertexts are the same.

- Typical application: secure transmission of short pieces of information (e.g. a temporary encryption key)

Example of ECB



Original Image

Encrypted image using ECB mode

Modes other than ECB result in pseudorandomness

Cipher Block Chaining (CBC)

- Solve security deficiencies in ECB
  - Repeated same plaintext block result different ciphertext block

- Each previous cipher blocks is chained to be input with current plaintext block, hence name

- Use Initial Vector (IV) to start process

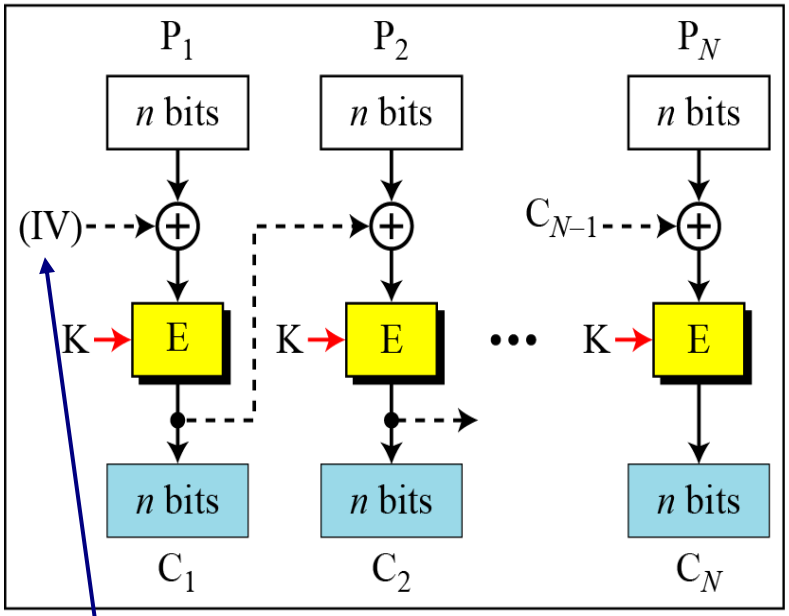
$$C_i = E_K (P_i \text{ XOR } C_{i-1})$$
$$C_0 = IV$$

Uses: bulk data encryption, authentication

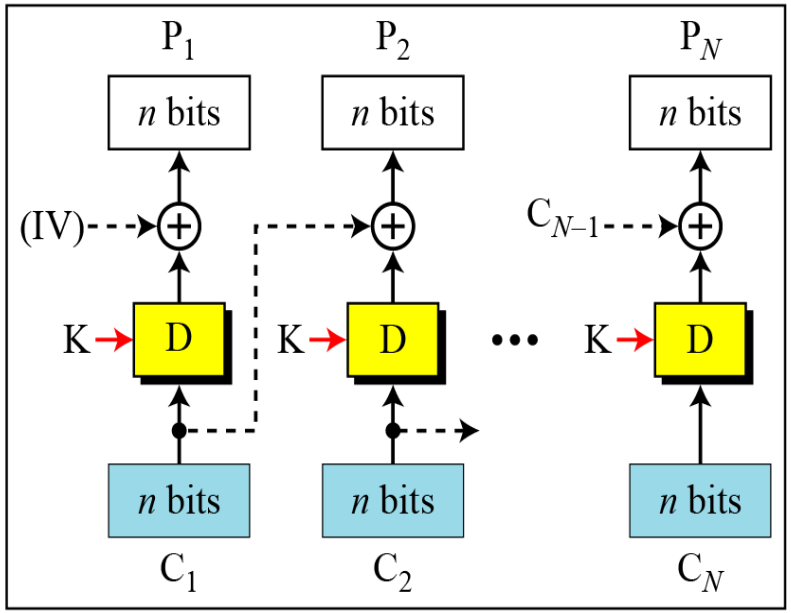
CBC scheme

E: Encryption
P_i: Plaintext block i
K: Secret key

D : Decryption
C_i : Ciphertext block i
IV: Initial vector (C_0)



Encryption



Decryption

Encryption:
$C_0 = IV$
$C_i = E_K (P_i \oplus C_{i-1})$

Decryption:
$C_0 = IV$
$P_i = D_K (C_i) \oplus C_{i-1}$

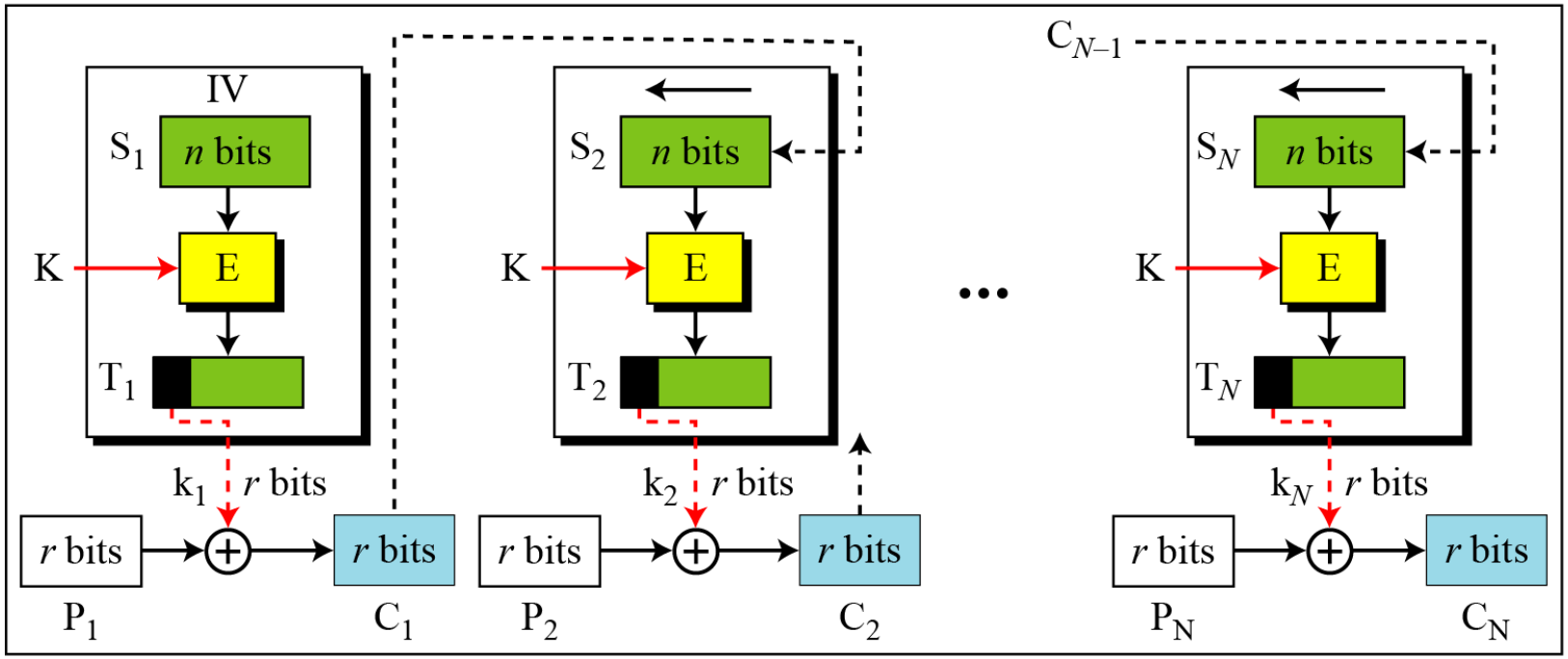
Cipher feedback mode (CFB) Scheme

Encryption: $C_i = P_i \oplus \text{SelectLeft}_r \{E_K [\text{ShiftLeft}_r (S_{i-1}) \mid C_{i-1})]\}$
Decryption: $P_i = C_i \oplus \text{SelectLeft}_r \{E_K [\text{ShiftLeft}_r (S_{i-1}) \mid C_{i-1})]\}$

E : Encryption
P_i: Plaintext block *i*
K: Secret key

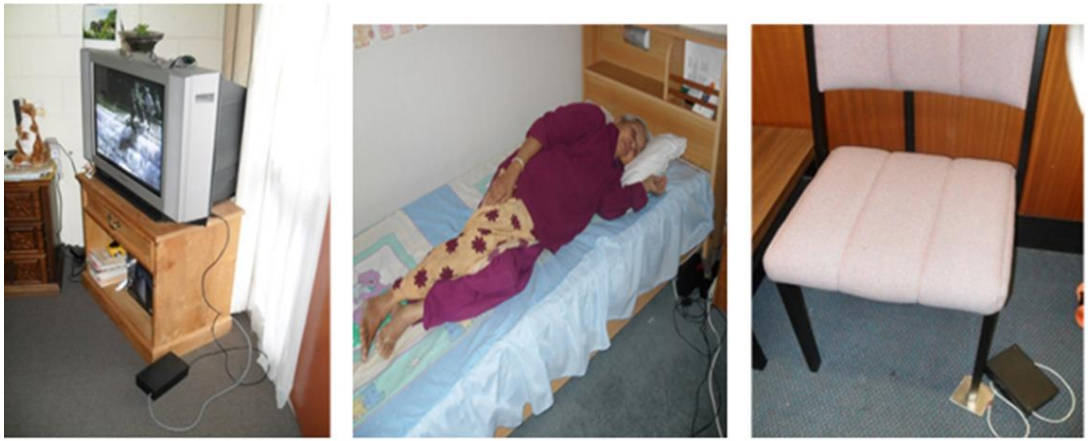
D : Decryption
C_i: Ciphertext block *i*
IV: Initial vector (S_1)

S_i: Shift register
T_i: Temporary register



Encryption

Example: Designing a Secure Smart Home



References

1. http://www.sfu.ca/~ljilja/ENSC427/News/Kurose_Ross/Chapter_8_V7.0_Accessible.pdf
2. Cryptography and Network Security: Principles and Practice 0133354695, 9780133354690.
3. A.K. Dewdney, The New Turning Omnibus, pp. 250-257, Henry Holt and Company, 2001.

Lnu.se