6G7Z1009: Introduction to Computer Forensics and Security

Cryptography - I

Acknowledgement and Reading List

- W. Stallings, Cryptography and Network Security: Principles and Practice (7th Edition), 2016, Pearson (Chapter 9&10)
- Nigel P. Smart, Cryptography Made Simple (Information Security and Cryptography), 2015, Springer
- M. Stamp, Information Security. Principles and Practice (2nd Edition), 2011, John Wiley (Chapter 4)
- D. Gollmann, Computer Security, 3rd Edition, 2011, John Wiley (Chapter 14 & 15)
- Alexander Stanoyevitch, Introduction to Cryptography with Mathematical Foundations and Computer Implementations, 2010, CRC Press (Chapter 9)
- J. Erickson, Hacking:The Art of Exploitation (2nd Edition), 2008 (Chapter 7)
- Online resources:
  - Menezes,A.,van Oorschot,P.,andVanstone,S.(1996) Handbook ofApplied Cryptography.CRC Press. Chapters 8 & 14. See http://www.cacr.math.uwaterloo.ca/hac/, [Online access 11 Sep. 2017].
  - Ellis, J.H. (1987) The history of Non-Secret Encryption. See http://www.cesg.gov.uk/site/publications/
  - media/ellis.pdf, [Online 10 September 2017].

Cryptography

- Cryptography is
  - The study of secret (crypto-) writing (-graphy)
  - The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form
- Concerned with the developing algorithms
  - Conceal the context of some message from all except the sender and recipient (privacy or secrecy), and/or
  - Verify the correctness of a message to the recipient (authentication)
  - Form the basis of many technological solutions to computer and communications security problems

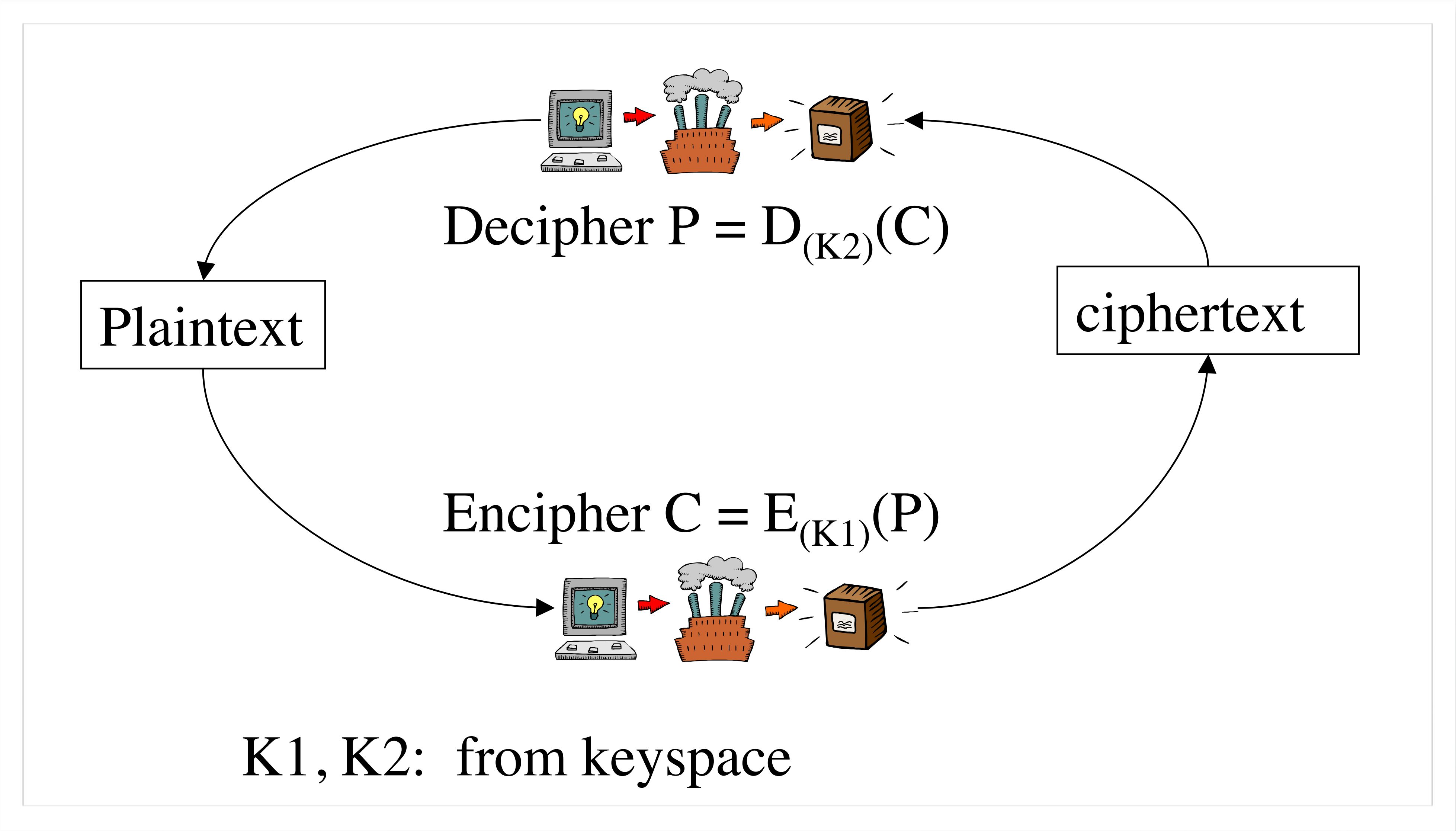
Cryptography-basic concepts

- Plaintext
  - The original intelligible message
- Ciphertext
  - The transformed message
- Key
  - Some critical information used by the cipher, known only to the sender & receiver
- Encipher (encode)
  - The process of converting plaintext to ciphertext

Cryptography-basic concepts

- Decipher (decode)
  - The process of converting ciphertext back into plaintext
- Cryptanalysis
  - The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called codebreaking
- Cryptology: Both cryptography and cryptanalysis
- Code: An algorithm for transforming an intelligible message into an unintelligible one using a code-book

Encryption and Decryption



Decipher P = $D_{(K2)}(C)$

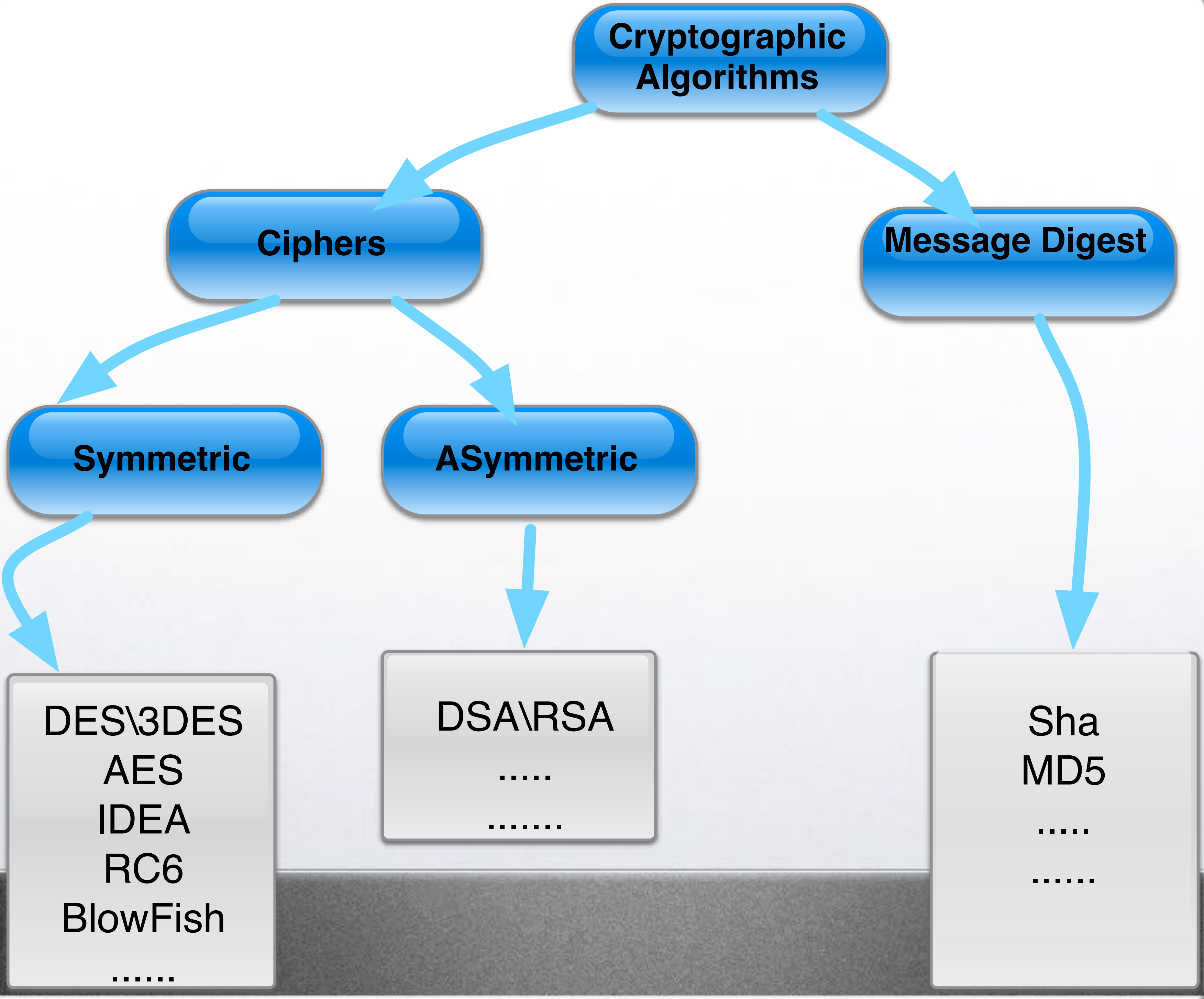
Plaintext

ciphertext

Encipher C = $E_{(K1)}(P)$

K1, K2: from keyspace

Cryptography



Cryptographic Algorithms

Ciphers

Message Digest

Symmetric

ASymmetric

DES\3DES
AES
IDEA
RC6
BlowFish
......

DSA\RSA
.....
....

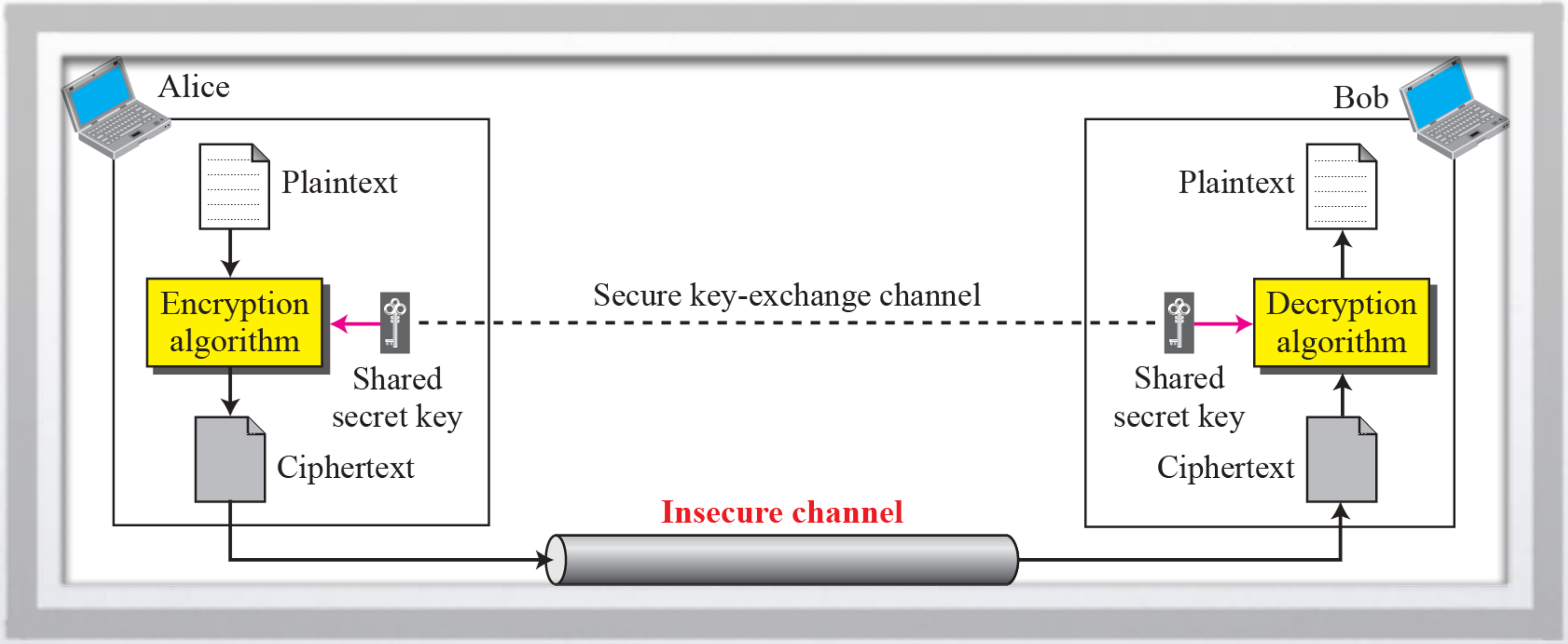
Sha
MD5
.....
......

Types of Security

- *Computational security:* which means that the best algorithm for breaking the cryptosystem requires a very large number of operations. e.g. AES.
- *Provable security*: which means that breaking the cryptosystem is at least as hard as solving some other difficult problem. e.g. RSA, Diffie-Hellman.
- *Unconditional security*: where the cryptosystem can never be broken even with infinite computational resources. e.g. One-time pad.

Traditional ciphers

- *Traditional ciphers are called symmetric-key ciphers (or secret-key ciphers) because the same key is used for encryption and decryption and the key can be used for bidirectional communication*

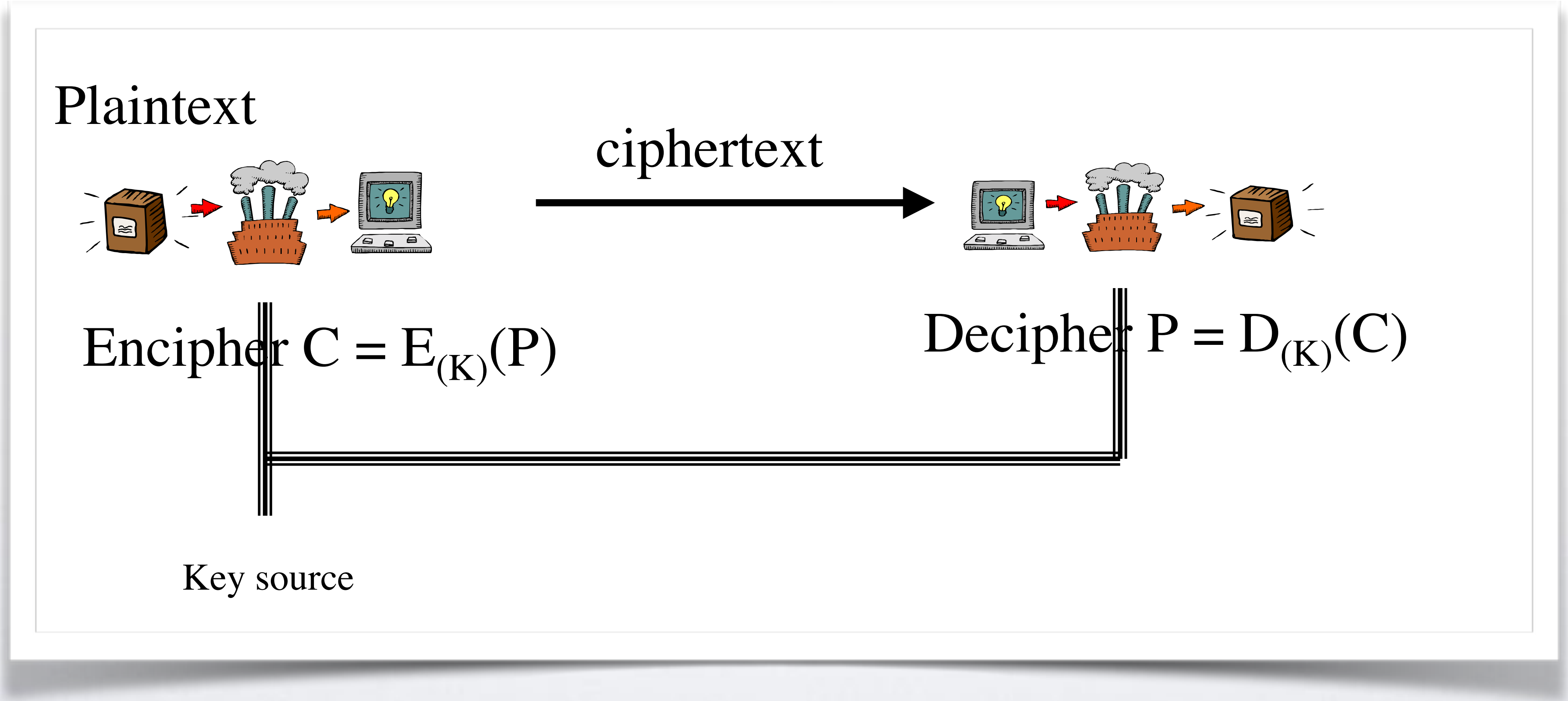


Source, Behrouz A.Forouzan, TCP/IP protocol suite (4th Edition), McGraw-Hill Higher Education, 2009

Traditional ciphers

- *Character-oriented traditional ciphers*
    - *Substitution: letters are replaced by other letters*
    - *Transposition: letters are arranged in a different order*
- *These ciphers may be:*
    - *Monoalphabetic: only one substitution/ transposition is used, or*
    - *Polyalphabetic: where several substitutions/ transpositions are used*

Traditional ciphers



Plaintext

ciphertext

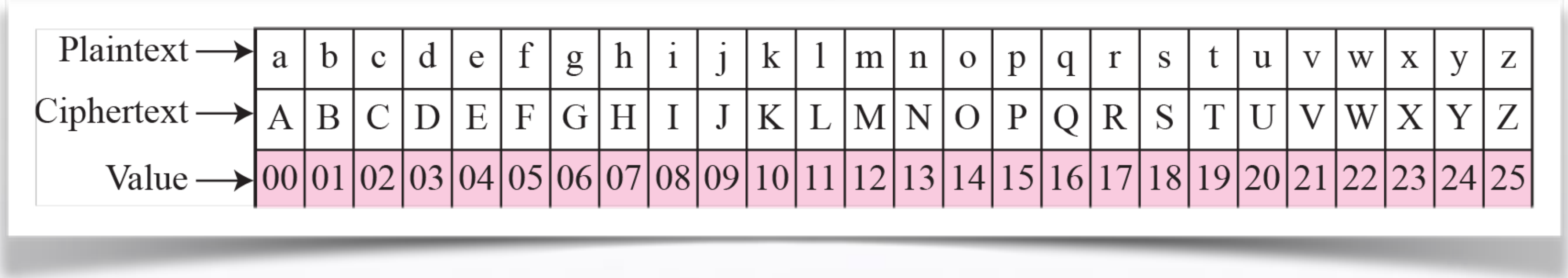
Encipher $C = E_{(K)}(P)$

Decipher $P = D_{(K)}(C)$

Key source

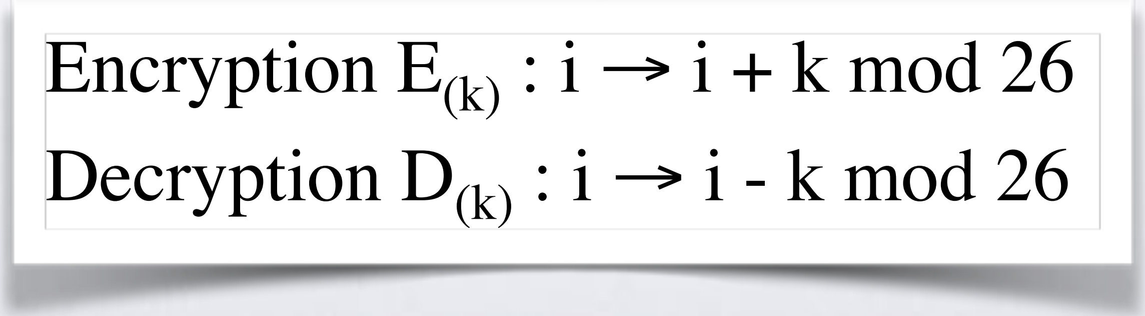
Traditional ciphers

- *Examples*
  - *Representation of characters in modulo 26*



Plaintext →	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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

  - *Mathematical model for encryption and decryption*



Encryption $E_{(k)} : i \rightarrow i + k \bmod 26$

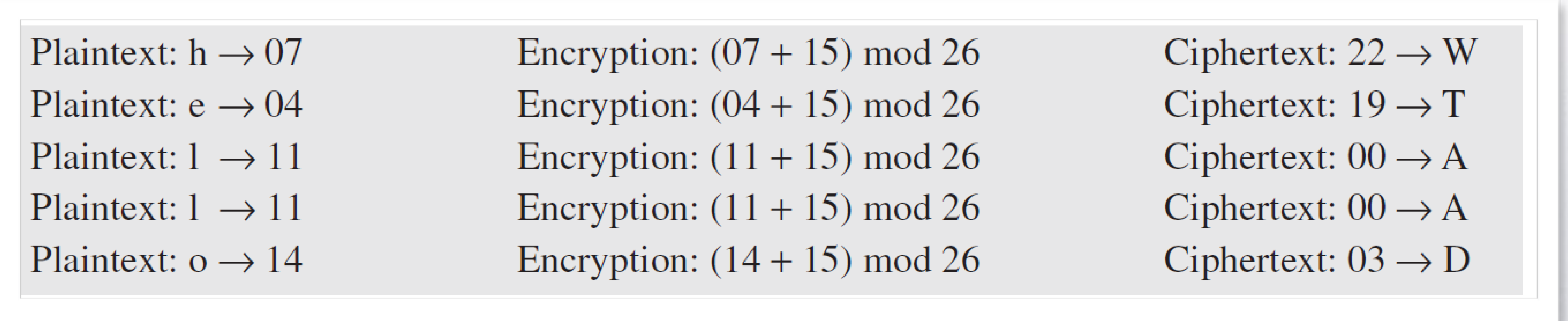
Decryption $D_{(k)} : i \rightarrow i - k \bmod 26$

Traditional ciphers

- *Examples*
  - *Use the additive cipher with key = 15 to encrypt the message "hello".*
  - *What is the answer?*

Traditional ciphers

- *Solution*
  - *We apply the encryption algorithm to the plaintext, character by character. The result is "WTAAD". Note that the cipher is monoalphabetic because two instances of the same plaintext character (ls) are encrypted as the same character (A).*



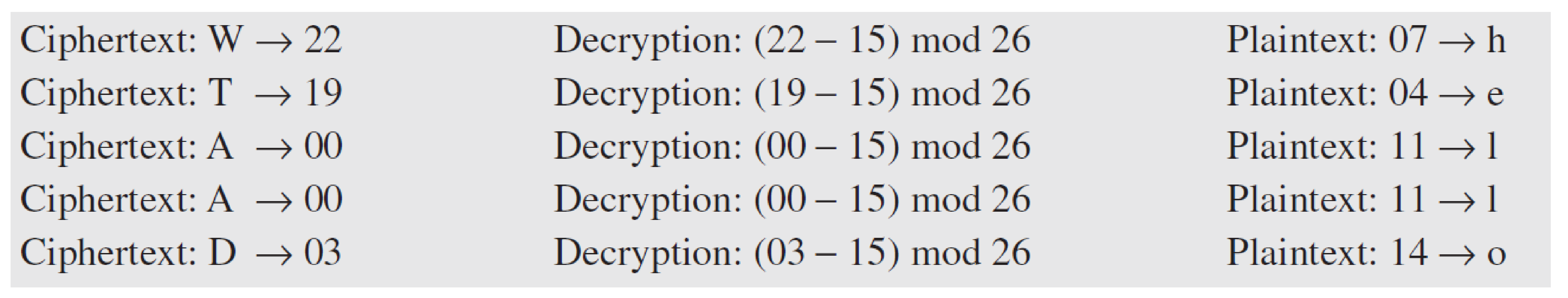
Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

Traditional ciphers

- *Example*
  - Use the additive cipher with key = 15 to decrypt the message “WTAAD”.
  - Can you work out?

Traditional ciphers

- *Examples*
    - We apply the decryption algorithm to the plaintext character by character. The result is “hello”. Note that the operation is in modulo 26, which means that we need to add 26 to a negative result (for example -15 becomes 11).



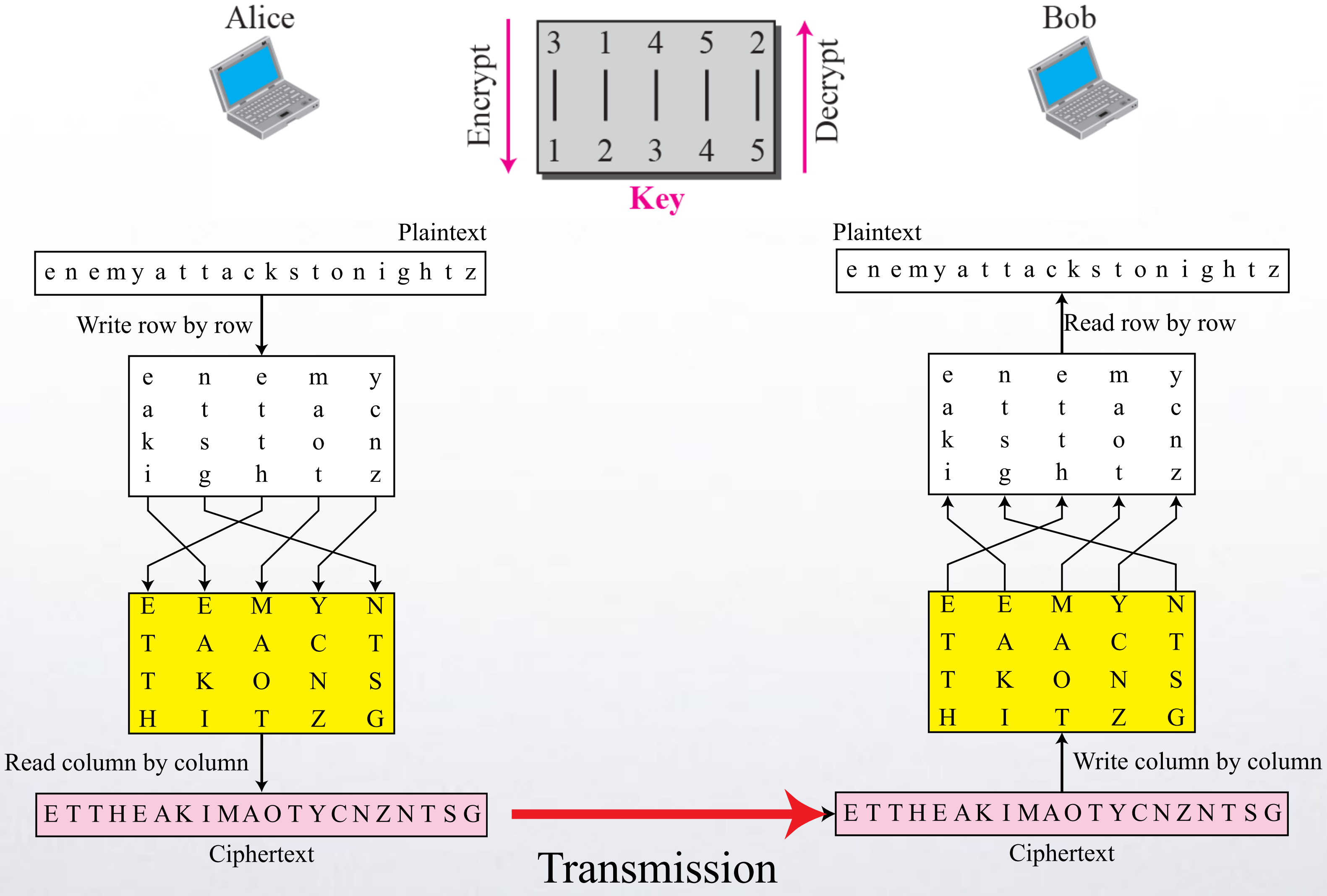
Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → o

Traditional ciphers

- *The examples given previously is " Caesar Cipher" examples, which Is one of the simplest and most widely known encryption techniques*

Traditional ciphers

- *Transposition cipher*



Alice

Bob

Encrypt

Decrypt

3	1	4	5	2
1	2	3	4	5

Key

Plaintext

enemyattackstonightz

Write row by row

e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	Z	G

Read column by column

ETTHEAKIMAOTYCNZNTSG

Ciphertext

Transmission

Plaintext

enemyattackstonightz

Read row by row

e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	Z	G

Write column by column

ETTHEAKIMAOTYCNZNTSG

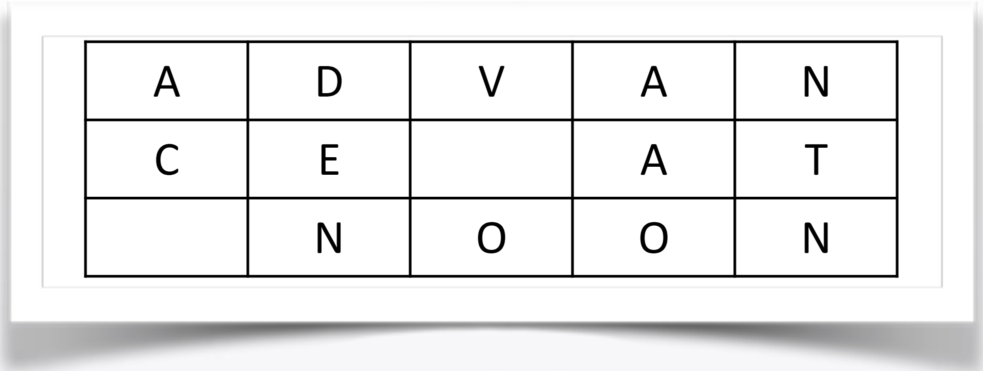
Ciphertext

Traditional ciphers

- *The order of the units is changed*
- *Mathematically a **bijective** function is used on the characters' positions to encrypt and an inverse function to decrypt*
- *Examples: Rail Fence cipher; Route cipher; Columnar transposition; Double transposition; Myszkowski transposition; Disrupted transposition; Grilles*

Traditional ciphers

- *Examples*
- *The message is placed row-wise in a 2D array (in this case 3x5 matrix) starting at top left.*

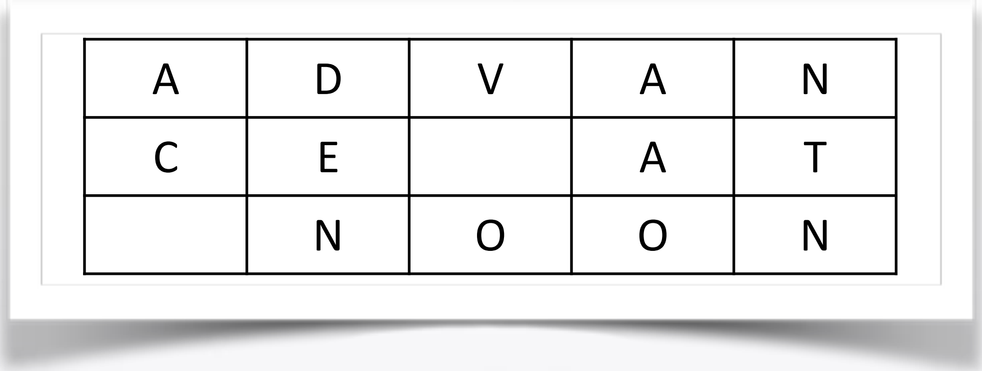


A	D	V	A	N
C	E		A	T
	N	O	O	N

- *The encrypted message is read out column-wise starting at the bottom right.*
- *So what is the encrypted message?*

Traditional ciphers

- *Examples*
- *The encrypted message is NTNOAAO VNED CA*



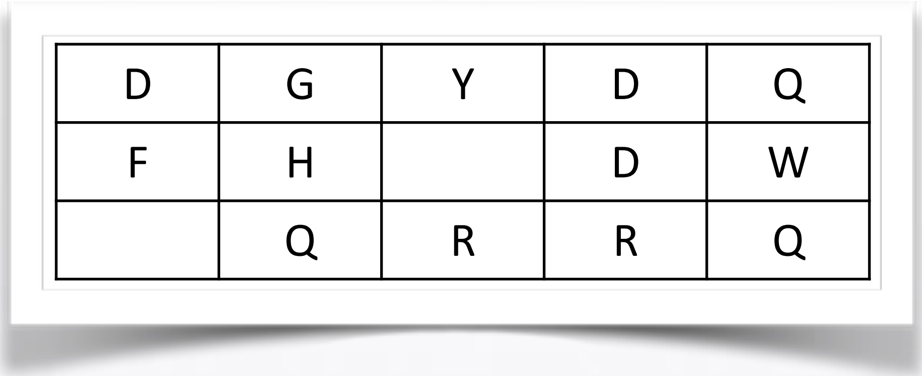
A	D	V	A	N
C	E		A	T
	N	O	O	N

Traditional ciphers

- *Product cipher:*
  - *Combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components to make it resistant to cryptanalysis*
    - *A sequence of simple transformations such as substitution, permutation, and modular arithmetic*
  - *The concept of product ciphers is due to Claude Shannon, who presented the idea in his foundational paper, Communication Theory of Secrecy Systems*

Traditional ciphers

- *Example:*
  - *Encrypting the output of the simple substitution cipher with the simple transposition cipher*



D	G	Y	D	Q
F	H		D	W
	Q	R	R	Q

  - *produces QWQRDDR YQHG FD*

Traditional ciphers

- *Some other traditional ciphers*
  - *ADFGVX Cipher*
  - *Alberti Cipher*
  - *Vigenère Cipher (https://www.youtube.com/watch?v=9zASwVoshiM)*
  - *Autokey Cipher, Beaufort Cipher, Polybius Cipher, ...*
  - *Look at a full list of traditional ciphers at here*

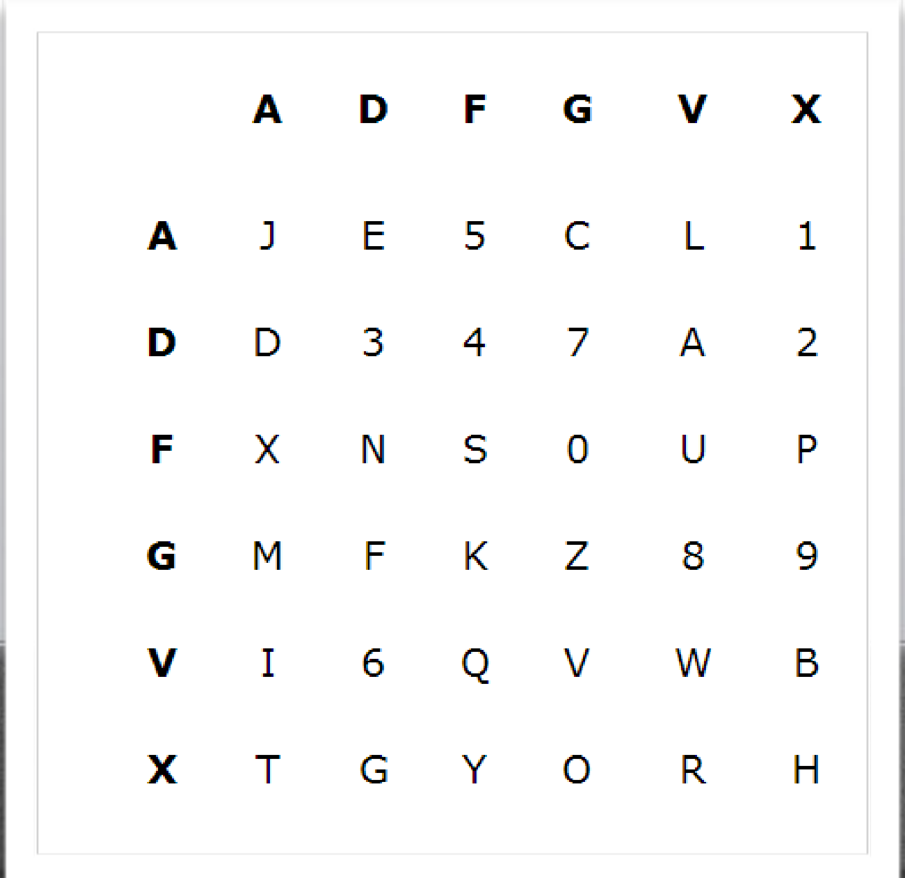
http://www.cryptool-online.org/index.php?option=com_content&view=article&id=47&Itemid=29&lang=en

Traditional ciphers

- *ADFGVX Cipher*
- *Messages are only composed of the characters A, D, F, G,V and X*
- *These characters have been chosen because they are easily distinguishable in the Morse alphabet*
- *The encoding consists of two phases: Phase 1: (substitution) Phase 2: (transposition)*

Traditional ciphers

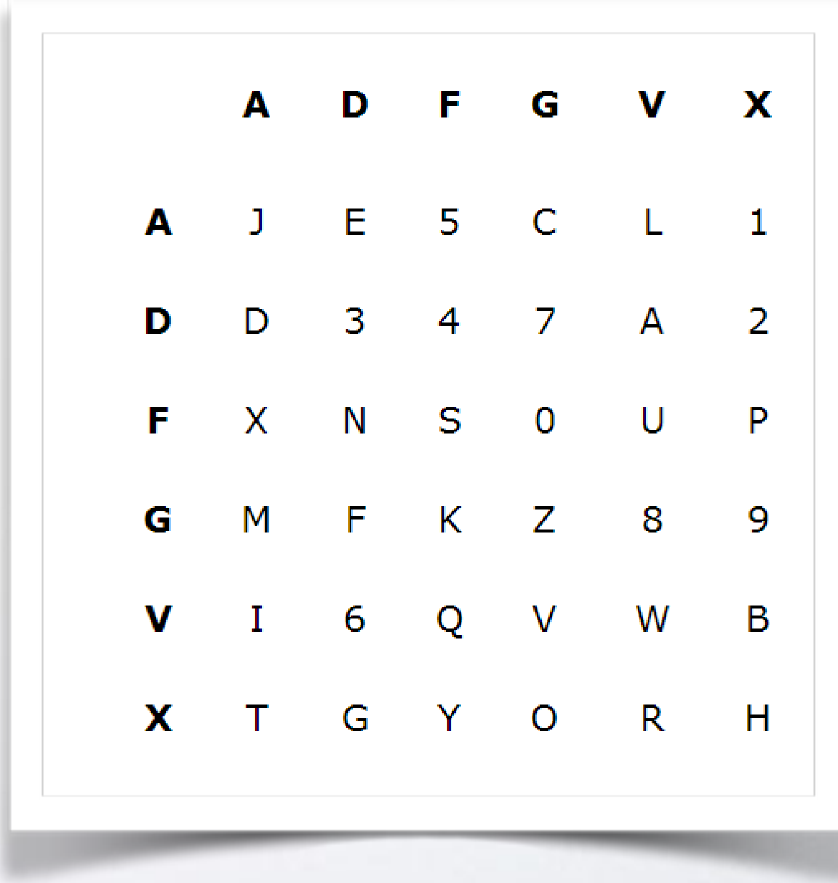
- *ADFGVX Cipher*
- *Phase 1: (substitution),A matrix with 6 rows and columns is formed*
- *Each character from the alphabet A-Z has to be written down in a 5x5 matrix as well as the numbers 0-9*



	A	**D**	**F**	**G**	**V**	**X**
A	J	E	5	C	L	1
D	D	3	4	7	A	2
F	X	N	S	0	U	P
G	M	F	K	Z	8	9
V	I	6	Q	V	W	B
X	T	G	Y	O	R	H

Traditional ciphers

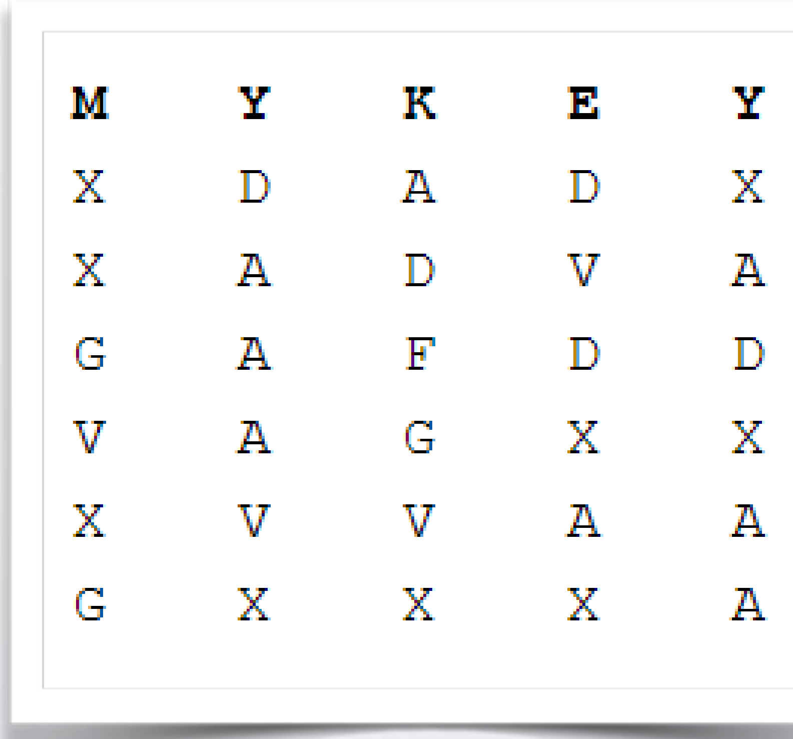
- *ADFGVX Cipher*
- *Phase 1: (substitution)*
- *For the message "GEHEIMNACHRICHT" the character G will be substituted according to the matrix shown right to XD. (row X and column D)*
- *After substituting all characters we get: "XD AD XX AD VA GA FD DV AG XX XV VAAG XX XA"*



	A	**D**	**F**	**G**	**V**	**X**
A	J	E	5	C	L	1
D	D	3	4	7	A	2
F	X	N	S	0	U	P
G	M	F	K	Z	8	9
V	I	6	Q	V	W	B
X	T	G	Y	O	R	H

Traditional ciphers

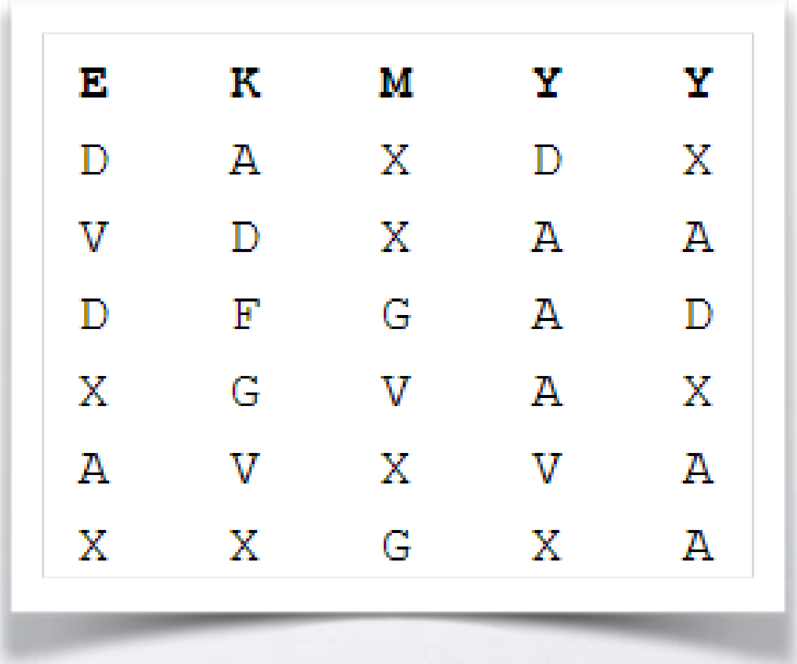
- *ADFGVX Cipher*
- *Phase 2: (transposition)*
- *An arbitrary keyword has to be chosen. E.g., "MYKEY”*
- *The matrix is read in row by row and read out column by column.*
- *Phase 1 output: "XD AD XX AD VA GA FD DV AG XX XV VA AG XX XA"*



M	**Y**	**K**	**E**	**Y**
X	D	A	D	X
X	A	D	V	A
G	A	F	D	D
V	A	G	X	X
X	V	V	A	A
G	X	X	X	A

Traditional ciphers

- *ADFGVX Cipher*
- *Phase 2: (transposition)*
- *For the last step, the columns are swapped*
- *To get the ciphertext, the matrix has to be read out column by column from the top to the bottom*
- *The final ciphertext would be: "DV DX AX AD FG VX XX GV XG DA AA VX XA DX AA"*



E	**K**	**M**	**Y**	**Y**
D	A	X	D	X
V	D	X	A	A
D	F	G	A	D
X	G	V	A	X
A	V	X	V	A
X	X	G	X	A

Modern ciphers

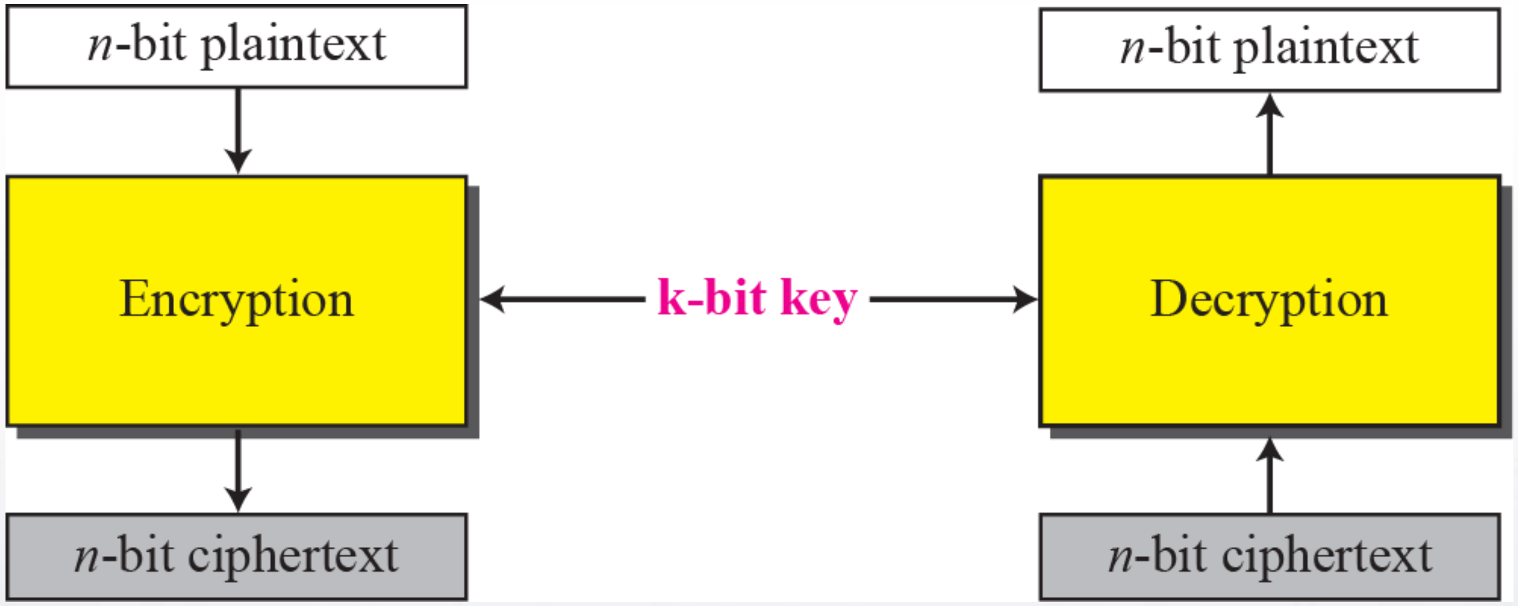
The traditional symmetric-key ciphers that we have studied so far are character-oriented ciphers. With the advent of the computer, we need bit-oriented ciphers. This is because the information to be encrypted is not just text; it can also consist of numbers, graphics, audio, and video data. It is convenient to convert these types of data into a stream of bits, to encrypt the stream, and then to send the encrypted stream. A modern block cipher can be either a block cipher or a stream cipher.

Modern ciphers

- Modern block ciphers
- Data encryption standards (DES)
- Modern stream ciphers

Modern ciphers-block ciphers

- Modern block ciphers



Modern ciphers-block ciphers

- Block ciphers
  - Is a type of symmetric-key encryption
  - Transforms a fixed-length block of plaintext data into a block of ciphertext data of the same length
  - This transformation takes place under the action of a user provided secret key
  - Decryption is performed by applying the reverse transformation to the ciphertext block using the same secret key
  - The fixed length is called the block size, and for many block ciphers, the block size is 64 bits

Modern ciphers-block ciphers

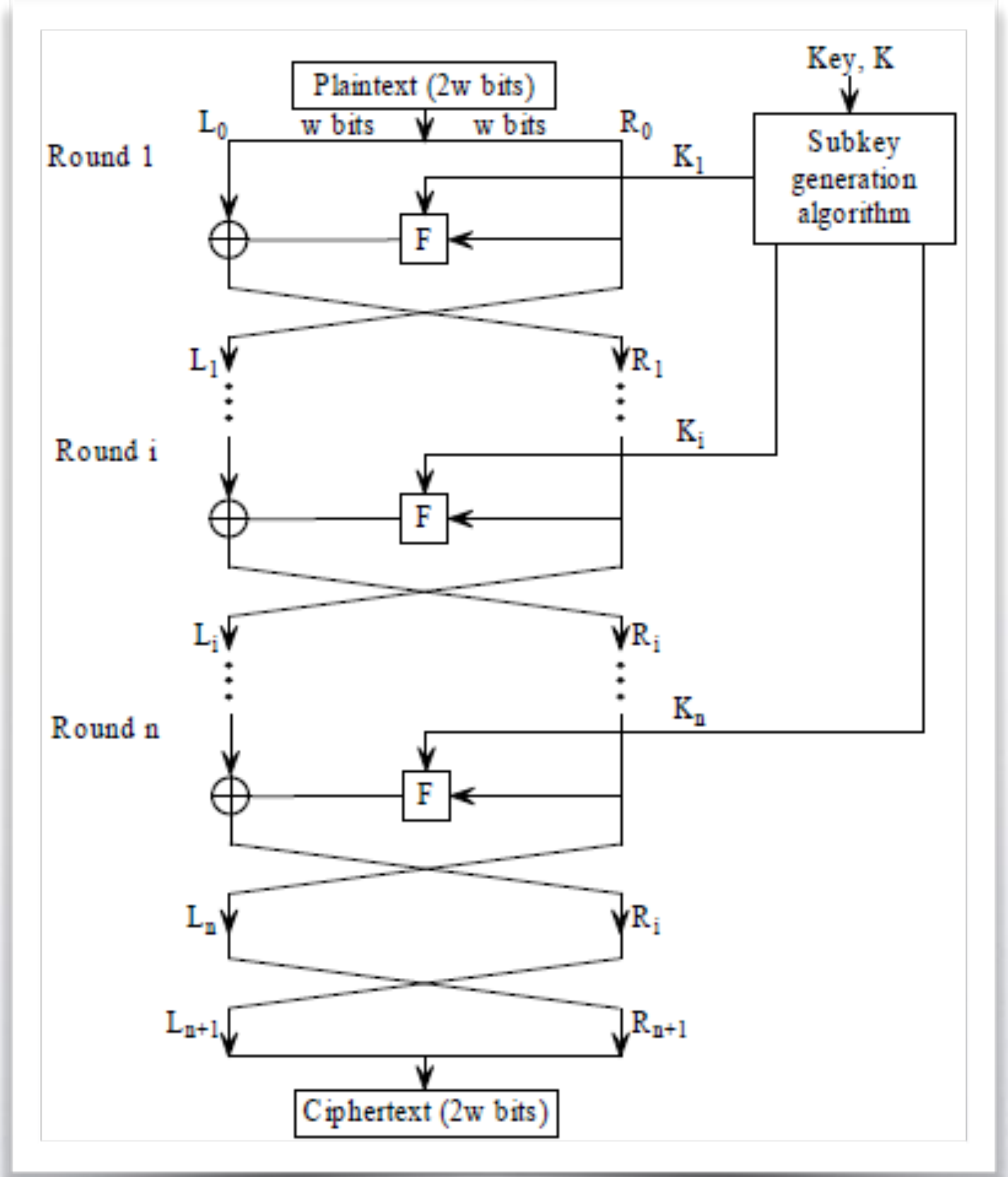
- Block Cipher Generic Example: Feistel Cipher Structure
  - Developed by Horst Feistel
  - Partitions input block into two halves
    - process through multiple rounds which
    - perform a substitution on left data half
    - based on round function of right half & sub-key
    - then have permutation swapping halves

Modern ciphers-block ciphers

- Feistel Cipher Structure
  - A plaintext block of width 2w is divided into two halves, L_0 and R_0
  - Each subsequent round, i, has inputs L_{i-1} and R_{i-1} derived from the previous round and a subkey K_i derived form the key K
  - All rounds have the same structure.
  - A round function parameterised by the subkey is used to generate a new right half by being applied to the present right half and then taking the exclusive OR with the left half
  - The new left half is simply the old right half.

Modern ciphers-block ciphers

- Feistel Cipher Structure



Modern ciphers-block ciphers

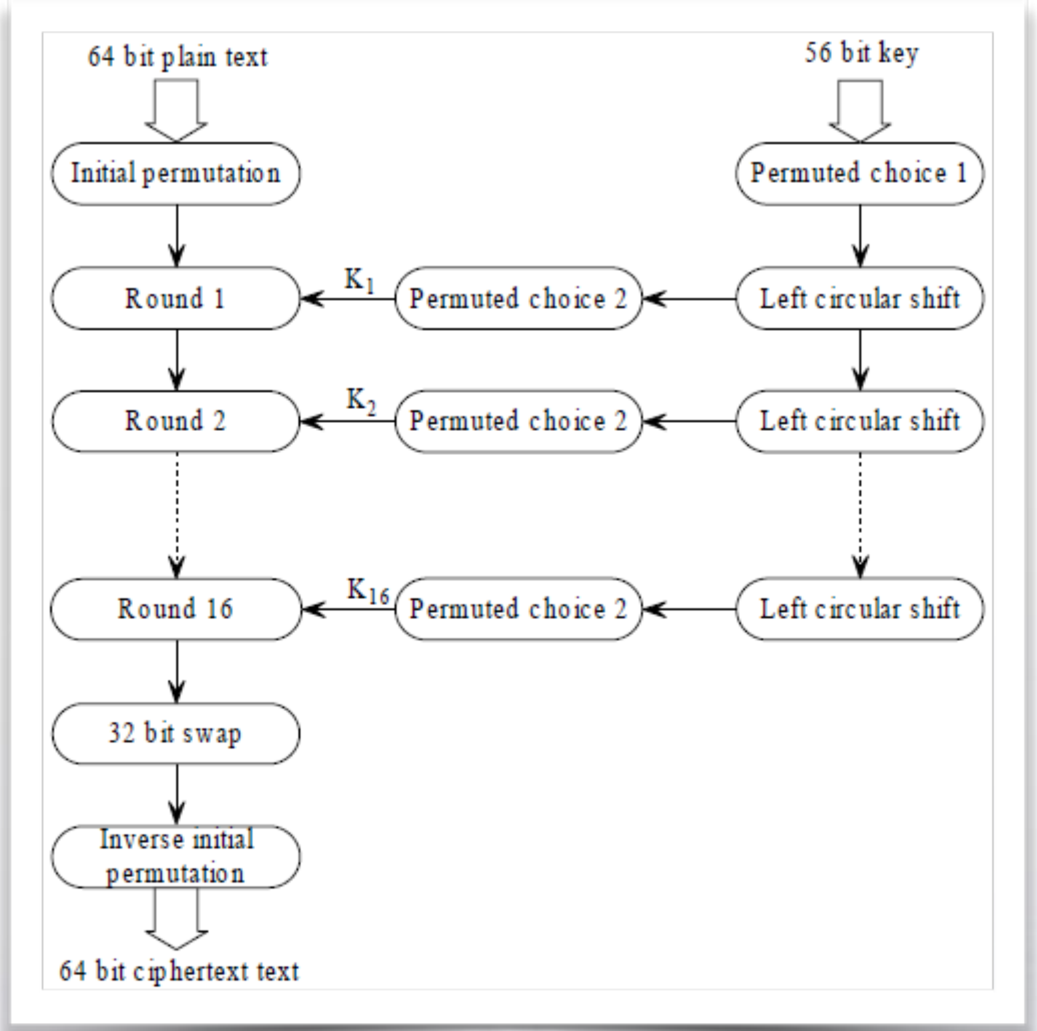
- As for any Feistel cipher can be described as:
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

Modern ciphers-block ciphers

- An example: DES(Data Encryption Standard), referring to the algorithm as the DEA (Data Encryption Algorithm).

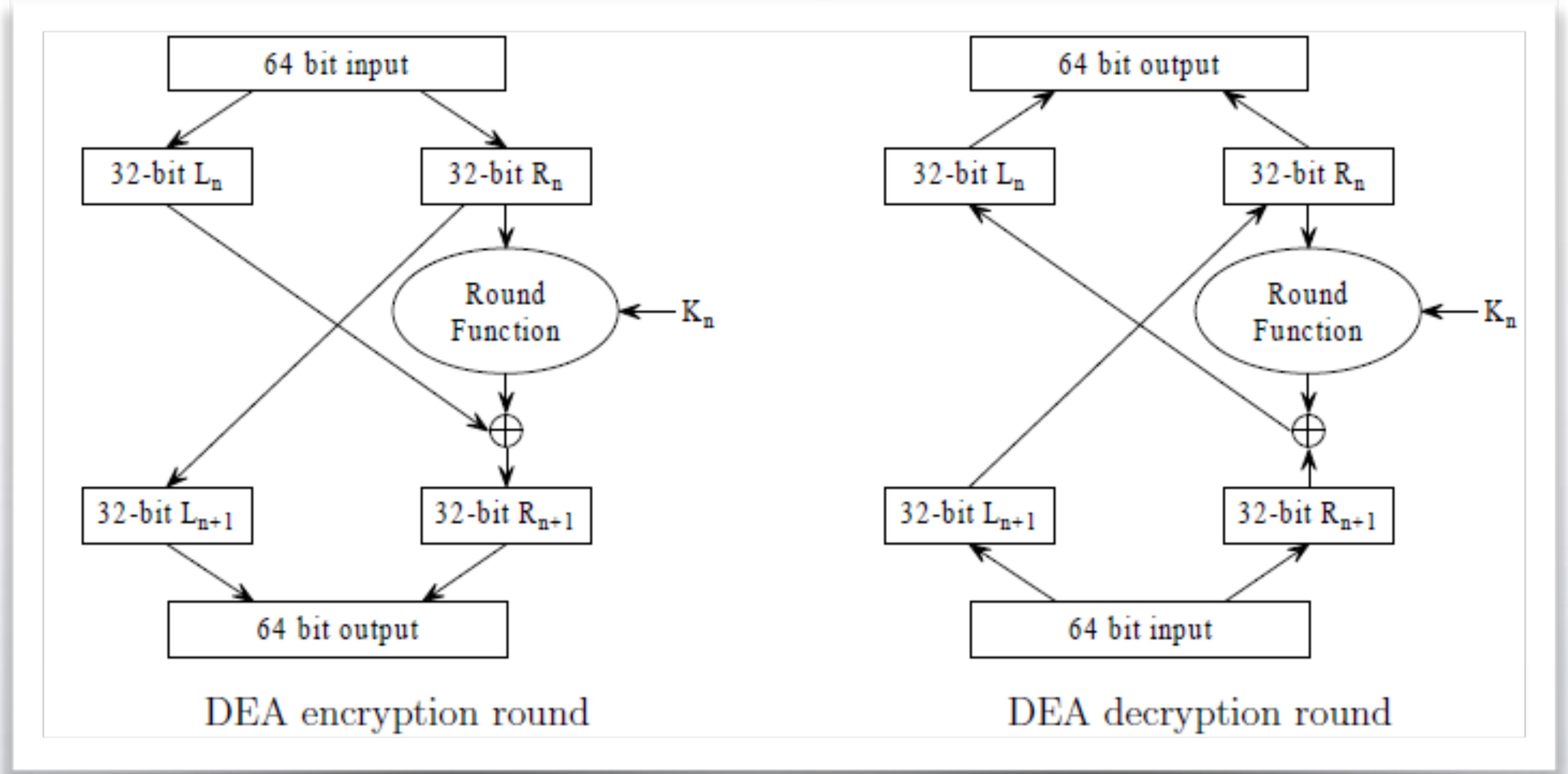
- The plaintext block size is 64 bits and the key is 56 bits long.

- After an initial permutation there are 16 rounds followed by swapping the left and right halves and then the inverse of the initial permutation is applied before the ciphertext block is output



Modern ciphers-block ciphers

- An example: DES(Data Encryption Standard)



Modern ciphers-block ciphers

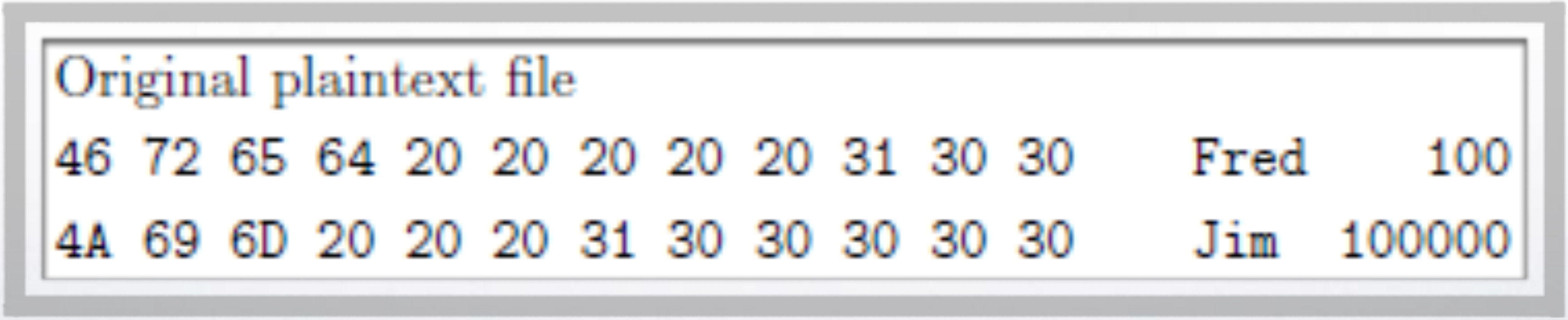
- The strength of DES - Key size
  - 56-bit keys have $2^{56} = 7.2 \times 10^{16}$ values
  - Brute force search looks hard
  - Recent advances have shown this is possible
    - in 1997 on Internet in a few months
    - in 1998 on dedicated h/w (EFF) in a few days
    - in 1999 above combined in 22hrs!
  - Still must be able to recognise plaintext
  - Must now consider alternatives to DES

Modern ciphers-block ciphers

- DES operation modes
    - ECB – Electronic Code Book
        - In ECB each 64 bit block of plaintext is simply encrypted a block at a time.
        - Thus if a message contains several identical 64 bit plaintext block this will show up as identical ciphertext blocks.
        - This is a weakness that it may be possible to exploit.

Modern ciphers-block ciphers

- Cut and Paste Attack on an ECB Encrypted File

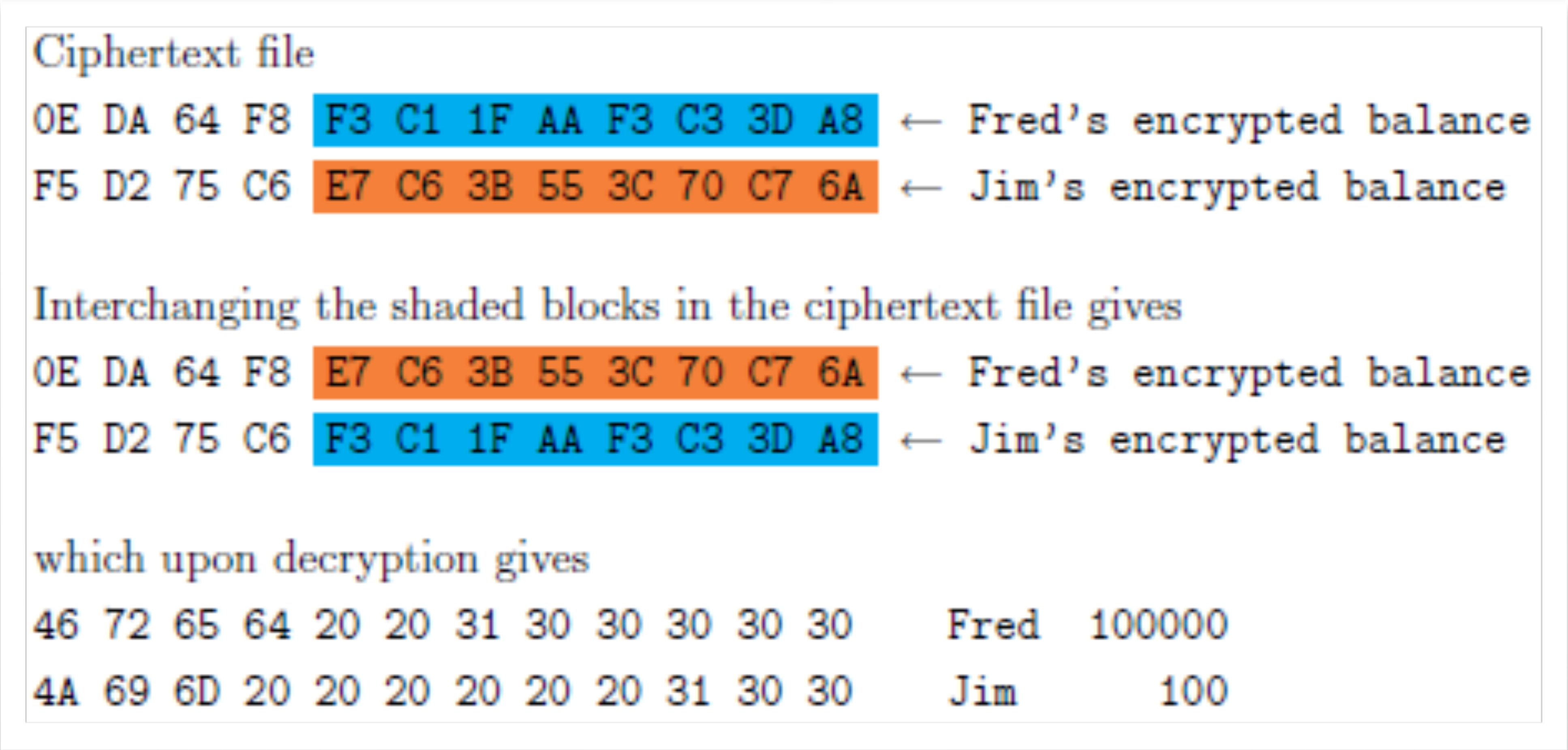


Original plaintext file

```
46 72 65 64 20 20 20 20 20 31 30 30    Fred    100
4A 69 6D 20 20 20 31 30 30 30 30 30    Jim  100000
```

Modern ciphers-block ciphers

- Cut and Paste Attack on an ECB Encrypted File



Ciphertext file

```
0E DA 64 F8 F3 C1 1F AA F3 C3 3D A8  ←  Fred's encrypted balance
F5 D2 75 C6 E7 C6 3B 55 3C 70 C7 6A  ←  Jim's encrypted balance
```

Interchanging the shaded blocks in the ciphertext file gives

```
0E DA 64 F8 E7 C6 3B 55 3C 70 C7 6A  ←  Fred's encrypted balance
F5 D2 75 C6 F3 C1 1F AA F3 C3 3D A8  ←  Jim's encrypted balance
```

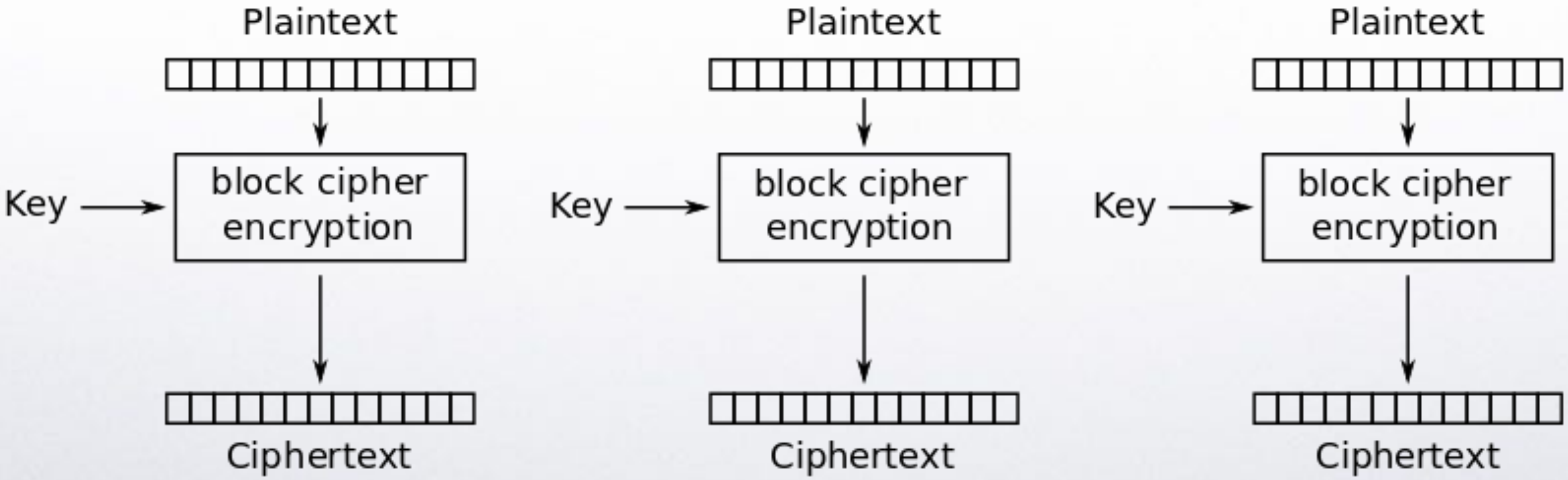
which upon decryption gives

```
46 72 65 64 20 20 31 30 30 30 30 30    Fred  100000
4A 69 6D 20 20 20 20 20 20 31 30 30    Jim      100
```

Modern ciphers-block ciphers

- DES operation modes

  - CBC – Cipher Block Chaining, Invented by IBM. each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.

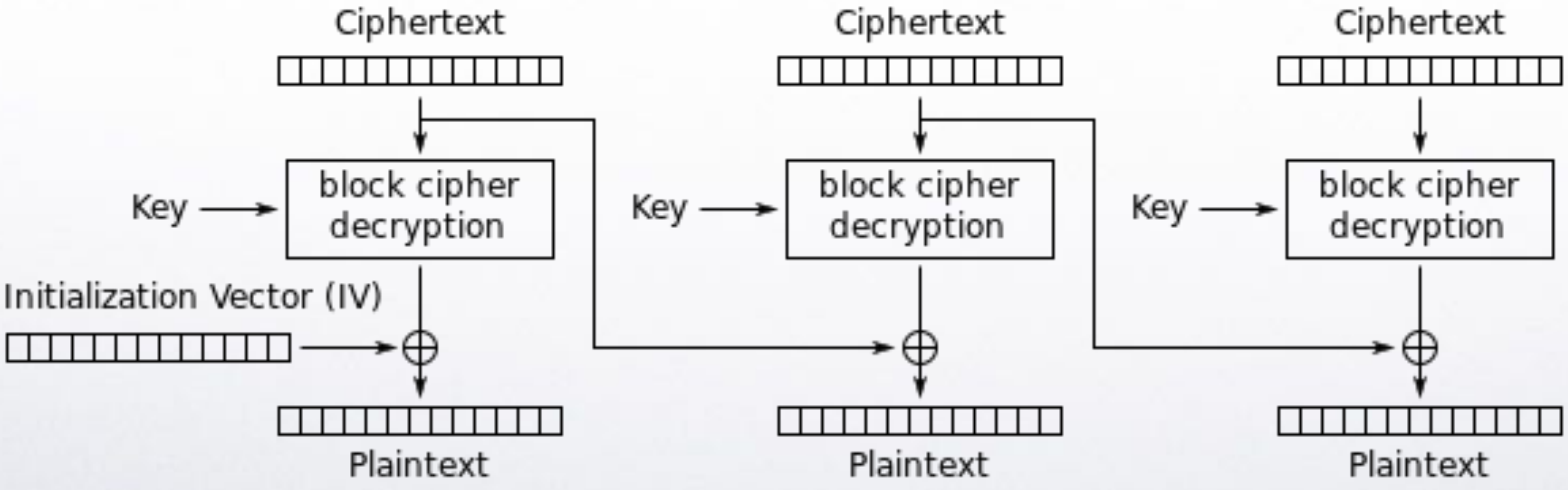


Electronic Codebook (ECB) mode encryption

http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Modern ciphers-block ciphers

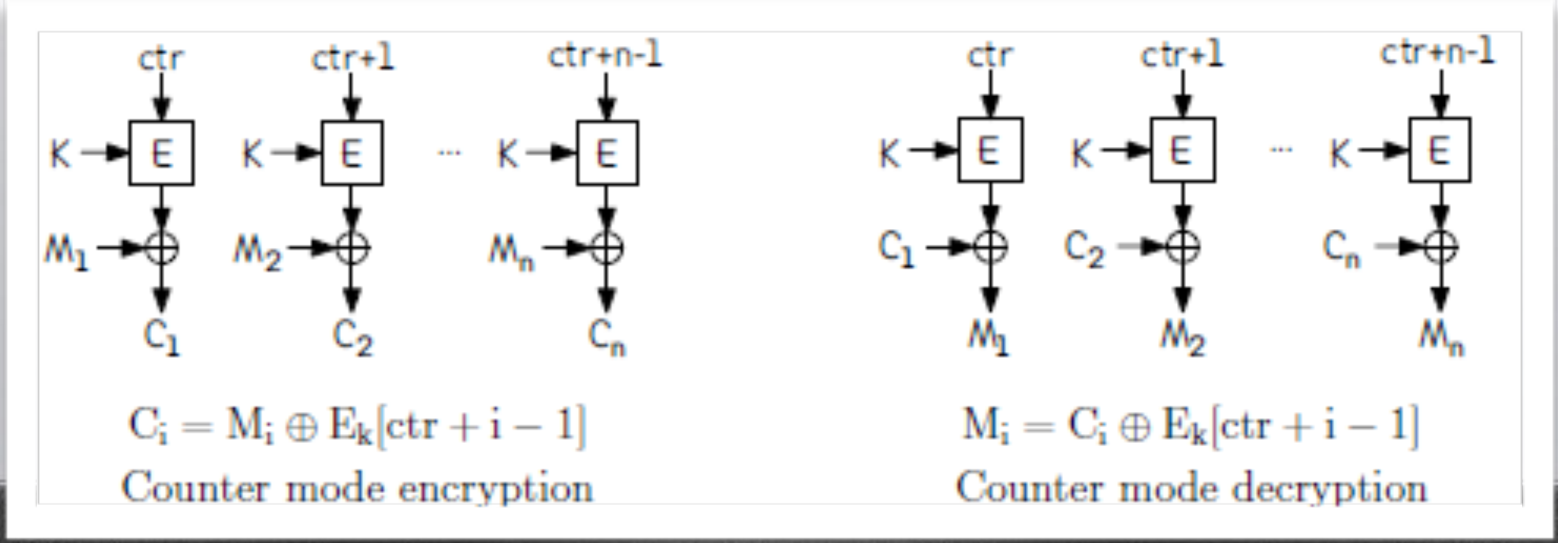
- DES operation modes
    - CBC – Cipher Block Chaining



Cipher Block Chaining (CBC) mode decryption

Modern ciphers-block ciphers

- DES operation modes- CTR – Counter mode
  - Counter mode essentially turns a block cipher into a stream cipher
  - Each plaintext block is encrypted by XORing it with the encrypted value of a “counter” (not Initialisation vector)
  - The counter may literally be a counter i.e. it increments by some fixed value e.g. 1 or it can be a simple function which produces a sequence which has a long period.



$C_i = M_i \oplus E_k[ctr + i - 1]$

Counter mode encryption

$M_i = C_i \oplus E_k[ctr + i - 1]$

Counter mode decryption

Modern ciphers-block ciphers

- DES operation modes- CTR – Counter mode
  - The advantages of counter mode in comparison with CBC are:
  - It can be parallelised.
  - Any cipher block can be decrypted without having to decrypt previous blocks.
  - Encrypted values of the counter can pre-calculated and stored.
  - Errors do not propagate.

Modern ciphers-block ciphers

- Modification of DES
  - Triple DES applies the DES cipher algorithm three times to each data block
  - The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible
  - Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

Modern ciphers-block ciphers

- Modification of DES
  - Triple DES uses a "key bundle" which comprises three DES keys, K_1, K_2 and K_3, each of 56 bits
  - The encryption algorithm is:

    ciphertext = $E_{K_3}(D_{K_2}(E_{K_1}(\text{plaintext})))$

    i.e., DES encrypt with K_1, DES decrypt with K_2, then DES encrypt with K_3.
  - Decryption is the reverse:

    plaintext = $DK1(E_{K_2}(D_{K_3}(\text{ciphertext})))$

    i.e., decrypt with K_3, encrypt with K_2, then decrypt with K_1.
  - Each triple encryption encrypts one block of 64 bits of data.

Modern ciphers-block ciphers

- Could we use double DES

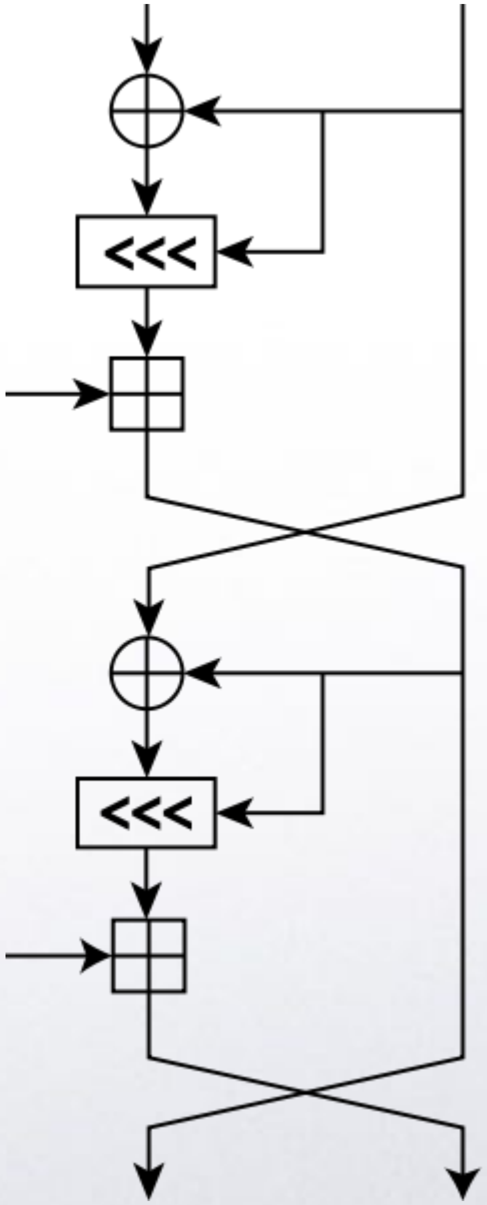
Is the length of the key Duplicated?

- On this model, we can expect that the effective length of the key is 2^{2n} where n represents the length in bits of k_1 and k_2 keys. However, this is not true.

- The size of the resulting key, indeed, in this case is equivalent to 2^{n+1}, an insignificant increase (just one bit) for a big value of n (typical) and it is not used for this reason.

Modern ciphers-block ciphers

- RC5
  - RC5 is a block cipher notable for its simplicity
  - Designed by Ronald Rivest in 1994
  - RC stands for "Rivest Cipher", or alternatively, "Ron's Code“
  - The Advanced Encryption Standard (AES) candidate RC6 was based on RC5
  - Unlike many schemes, RC5 has a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255).
  - A key feature of RC5 is the use of data-dependent rotations
  - The general structure of the algorithm is a Feistel-like network



Modern ciphers - stream ciphers

- A stream cipher generates what is called a keystream (a sequence of bits used as a key)

- Encryption is accomplished by combining the **keystream** with the plaintext, usually with the bitwise **XOR** operation

- The generation of the keystream can be independent of the plaintext and ciphertext, yielding what is termed as **synchronous**

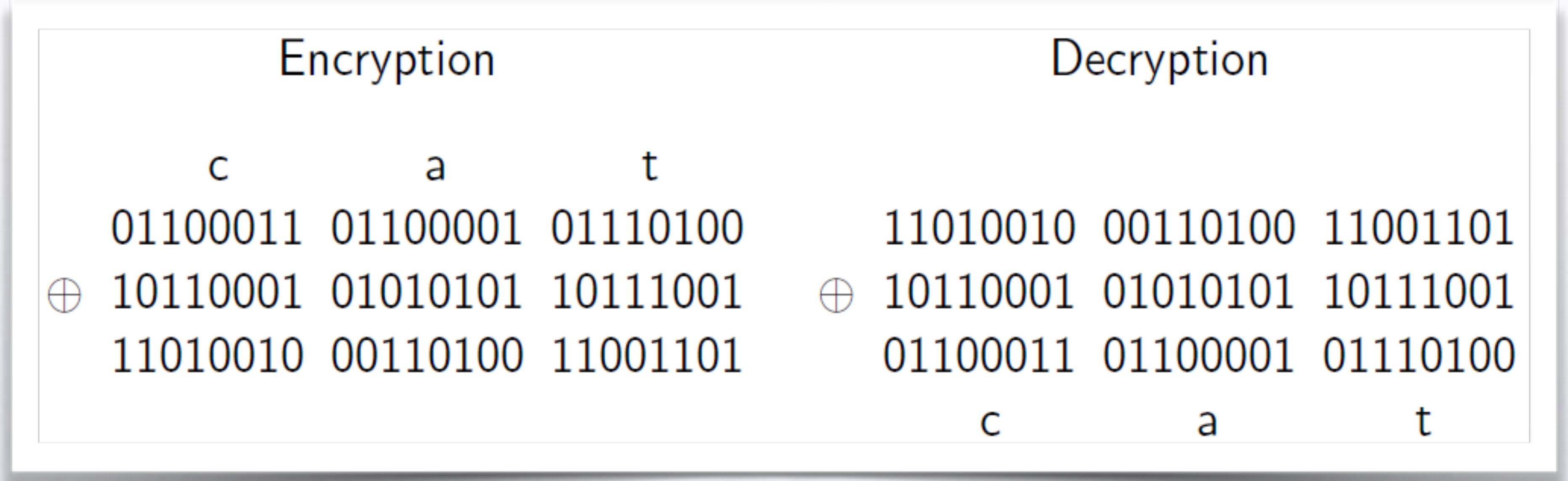
- Or it can depend on the data and its encryption, in which case the stream cipher is said to be **self-synchronising**.

- Most stream cipher designs are for synchronous stream ciphers.

Modern ciphers - stream ciphers

- Stream cipher example: Vernam Cipher

- A Vernam cipher is a stream cipher in which the plaintext is XORed with a random or pseudorandom stream of data of the same length to generate the ciphertext. If the stream of data is truly random and used only once, then the cipher is a one-time pad.



Encryption

	c	a	t
	01100011	01100001	01110100
⊕	10110001	01010101	10111001
	11010010	00110100	11001101

Decryption

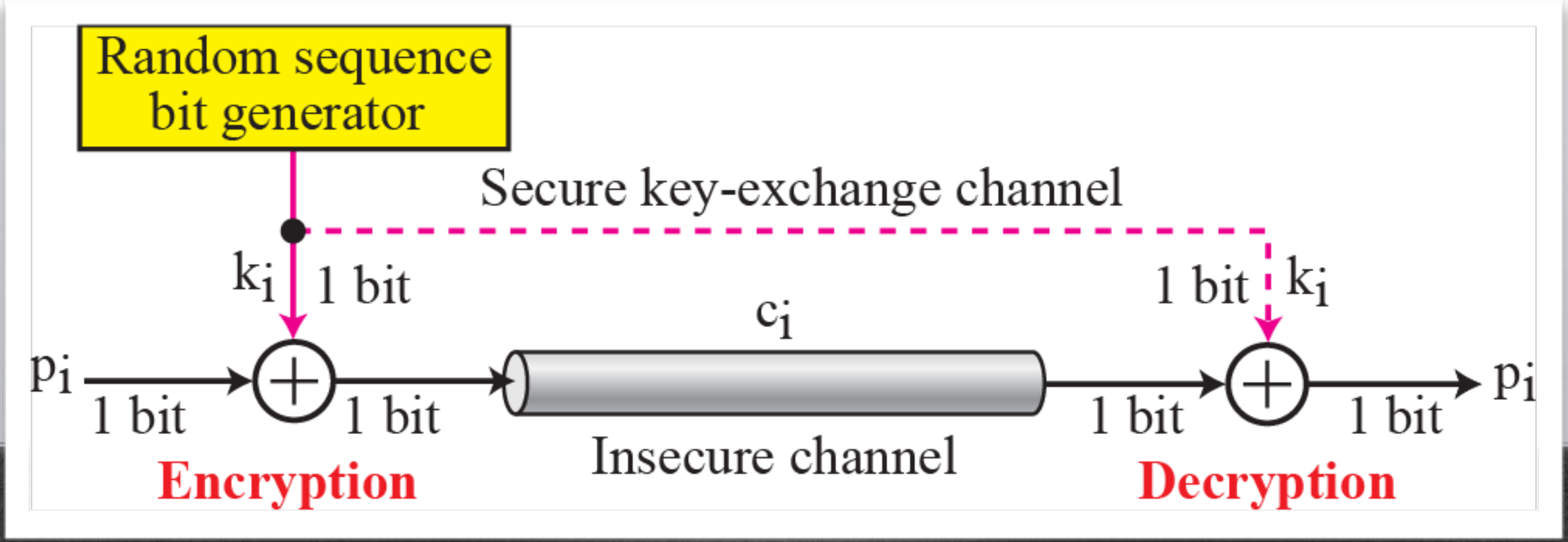
	11010010	00110100	11001101
⊕	10110001	01010101	10111001
	01100011	01100001	01110100
	c	a	t

Modern ciphers -one time pad

- The one time pad is an encryption algorithm that can be proved to be perfectly secure.

- The message is encrypted by combining (usually XORing) it with a perfectly random key at least as long as the message and the key is only used once.

- Apart from the problem of obtaining a perfectly random key (you cannot generate them on a computer) the main problem with one time pads is the distribution of keys.



Stream ciphers vs. Block ciphers

- Stream cipher
  - A type of symmetric encryption algorithm
  - Can be designed to be exceptionally fast, much faster than any block cipher.
  - Typically operate on smaller units of plaintext, usually bits. With a stream cipher, the transformation of plaintext units will vary, depending on when they are encountered during the encryption process.
- Block ciphers
  - Operate on large blocks of data, stream ciphers
  - The encryption of any particular plaintext with will result in the same ciphertext when the same key is used

Summary

- Cryptography:
  - Properties of security ciphers
  - Basic concepts
  - Traditional ciphers/modern ciphers
  - Block vs stream ciphers