Computer security

Section 4

Eng. Ahmed Safar

One-time Pad cipher

❑ problems in generation & safe distribution of key

❑ Key is a random string that is at least as long as the plaintext, the cipher will be secure

❑ Fix the vulnerability of the mono-alphabetical substitution cipher by encrypting letters in different locations differently

Example 1

plaintext: come today

key : ncbtzqarx

Answer

Plaintext	c	o	m	e	t	o	d	a	y
P#	2	14	12	4	19	14	3	0	24
K	**N**	**C**	**B**	**T**	**Z**	**Q**	**A**	**R**	**X**
K#	13	2	1	19	25	16	0	17	23
total	15	16	13	23	44	30	3	17	47
C#	15	16	13	23	18	4	3	17	21
Cipher text	P	Q	N	X	S	E	D	R	V

Example 2

plaintext: meet me outside

key : bdufghweiufgw

Answer

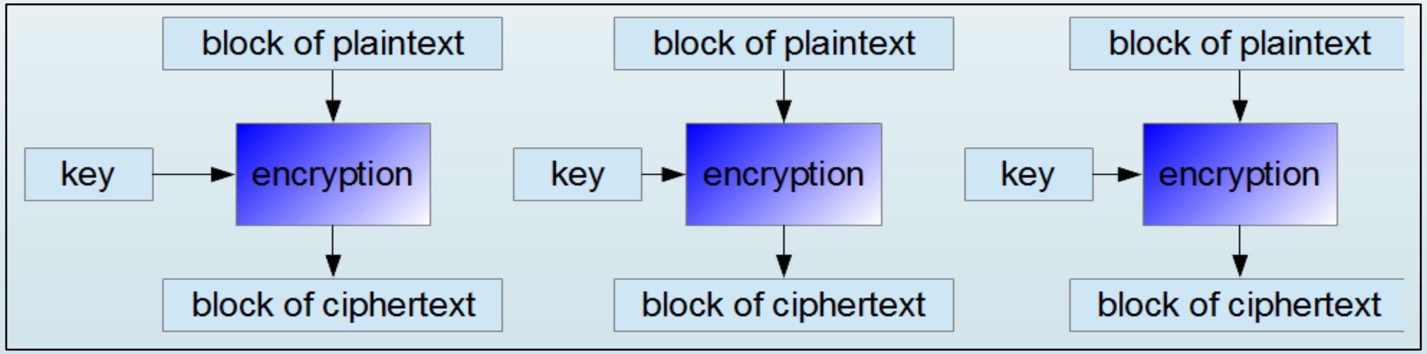
Plaint text	**m**	**e**	**e**	**t**	**m**	**e**	**o**	**u**	**t**	**s**	**i**	**d**	**e**
P#	12	4	4	19	12	4	14	20	19	18	8	3	4
K	**b**	**d**	**u**	**f**	**g**	**h**	**w**	**e**	**i**	**u**	**f**	**g**	**w**
K#	1	3	20	5	6	7	22	4	8	20	5	6	22
total	13	7	24	24	18	11	36	24	27	38	13	9	26
C#	13	7	24	24	18	11	10	24	1	12	13	9	0
Cipher text	N	H	Y	Y	S	L	K	Y	B	M	N	J	A

Block Ciphers modes of operation

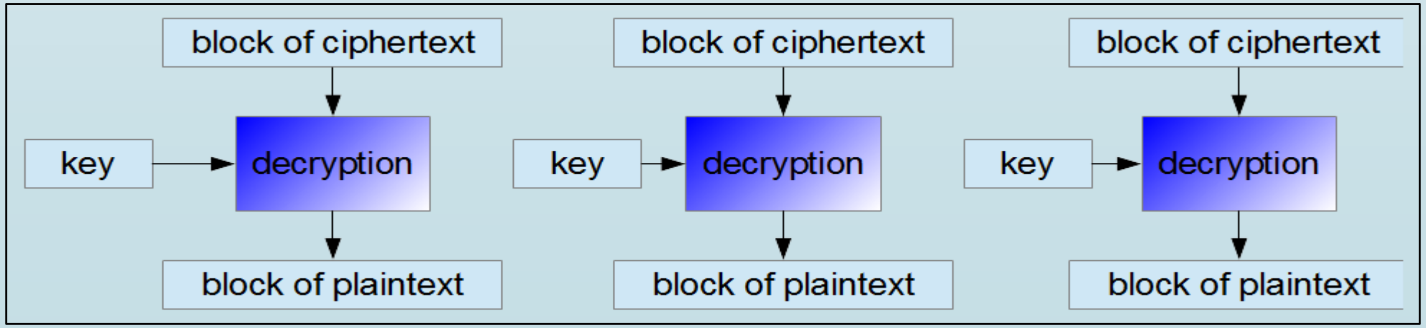
1) ECB (electronic codebook) Mode

- It is the simplest mode of encryption.
- Each plaintext block is encrypted separately.
- Similarly, each cipher text block is decrypted separately.

Encryption



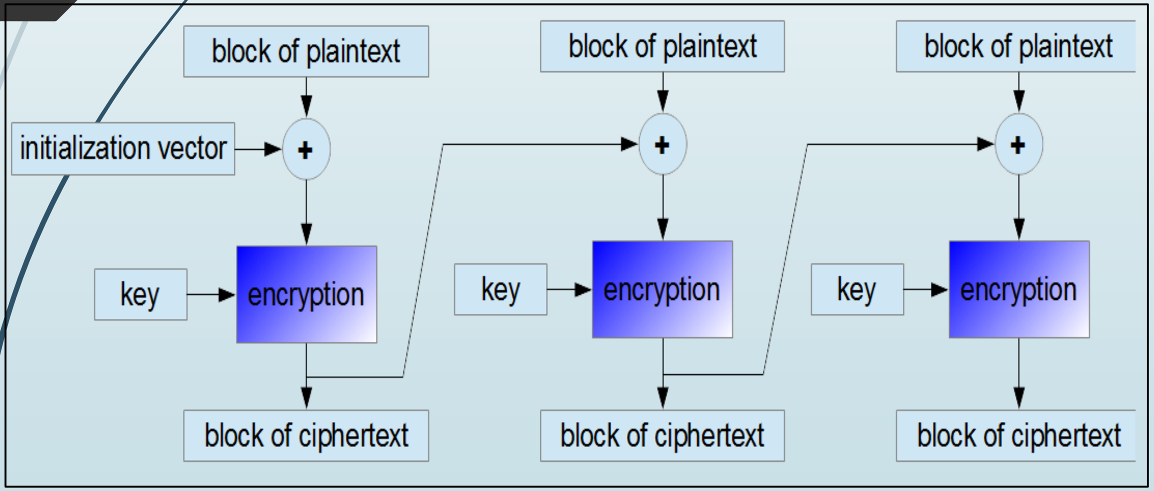
Decryption



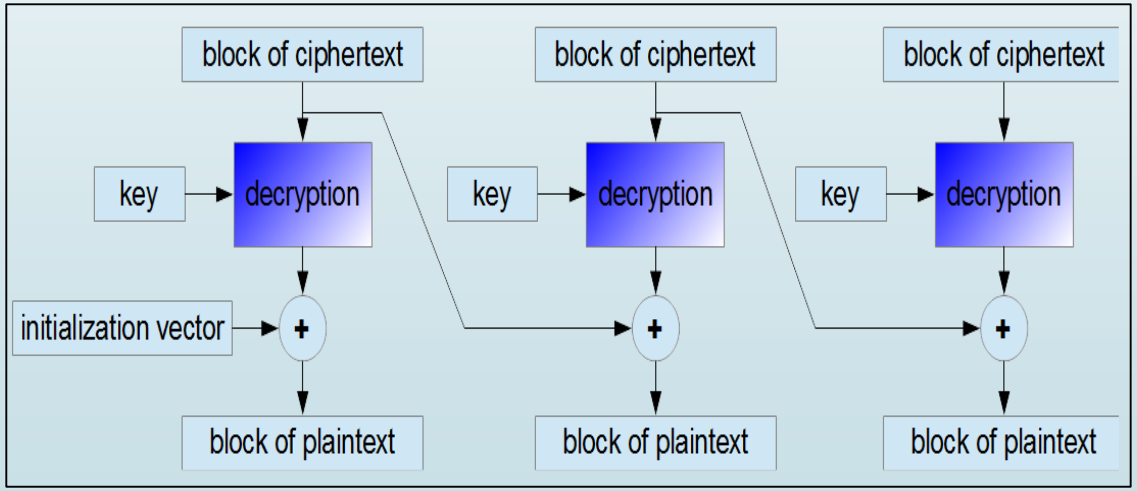
2) CBC (cipher-block chaining) Mode

❖adding XOR each plaintext block to the ciphertext block that was previously produced.

❖The result is then encrypted using the cipher algorithm in the usual way.



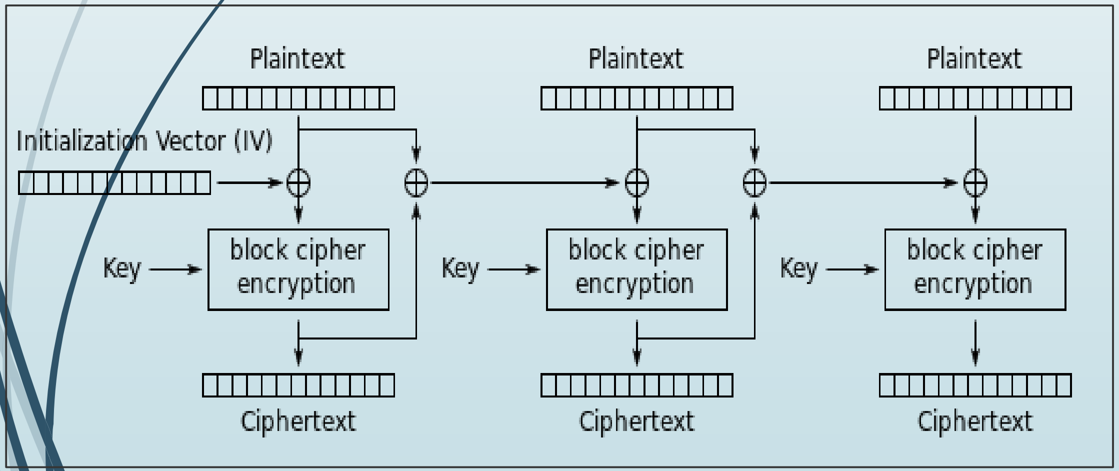
Encryption



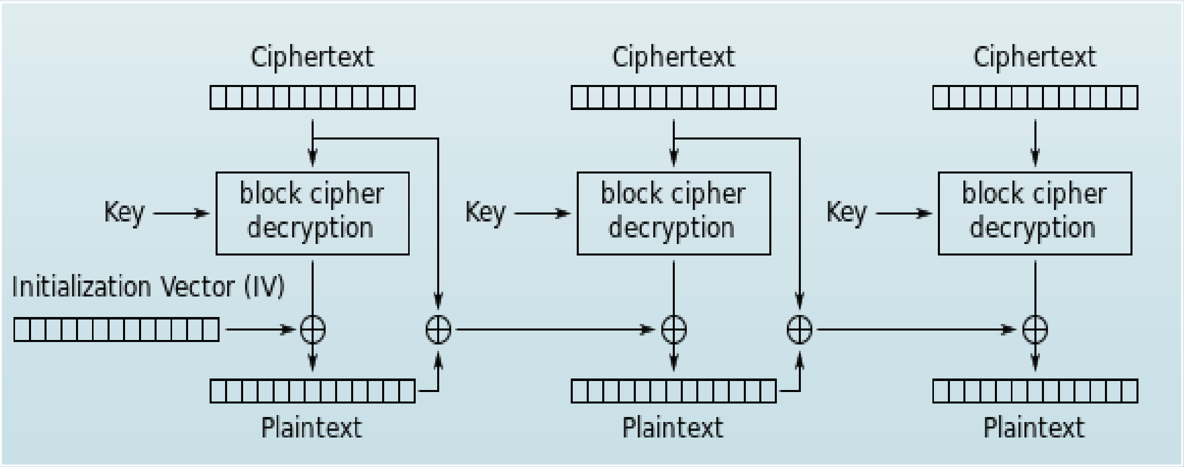
Decryption

3) PCBC (propagating or plaintext cipher-block chaining) Mode

- ❑ The PCBC mode is similar to the CBC mode
- ❑ It also mixes bits from the previous and current plaintext blocks, before encrypting them



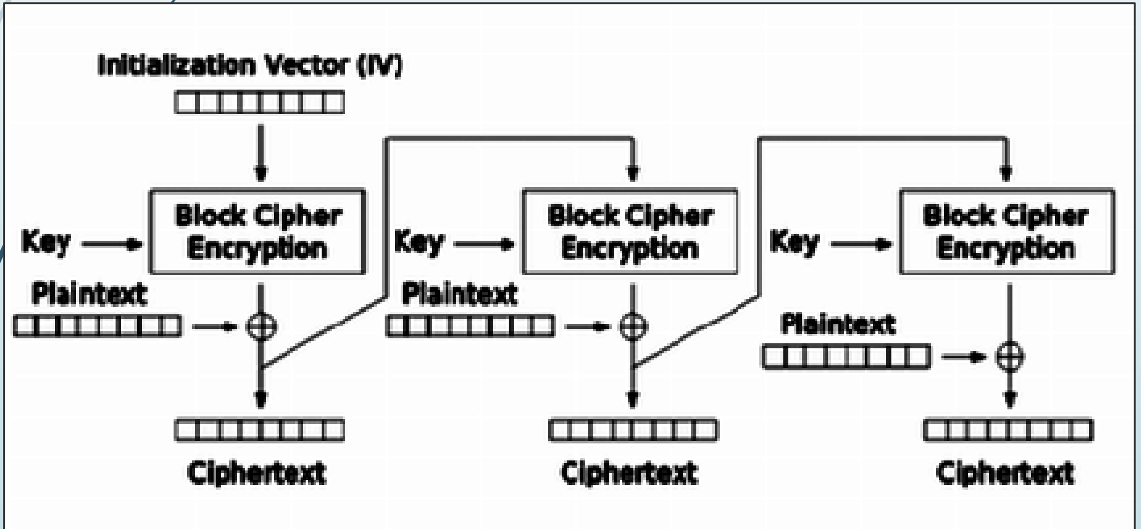
Encryption



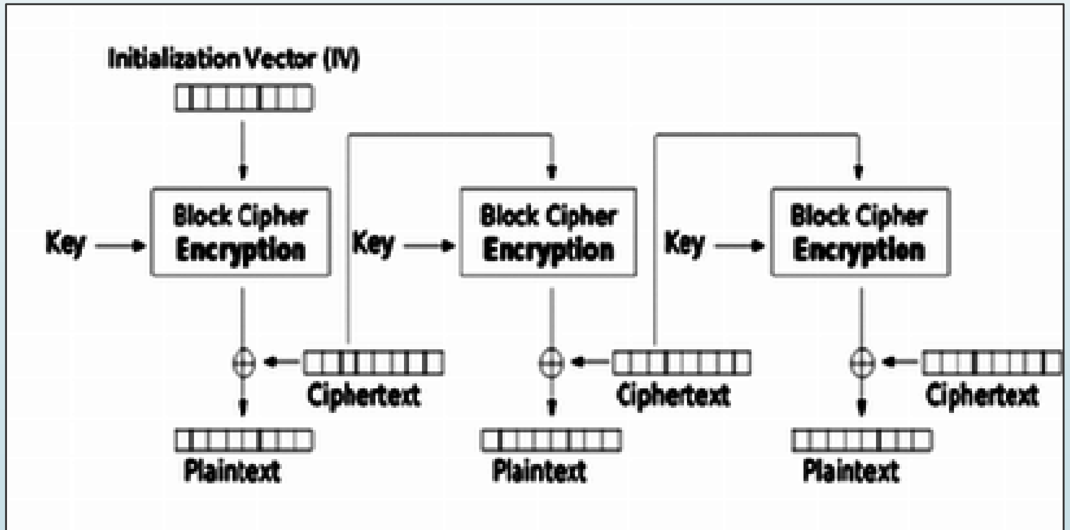
Decryption

4) CFB (cipher feedback) Mode

- Encrypt ciphertext data from the previous round and then add the output to the plaintext bits



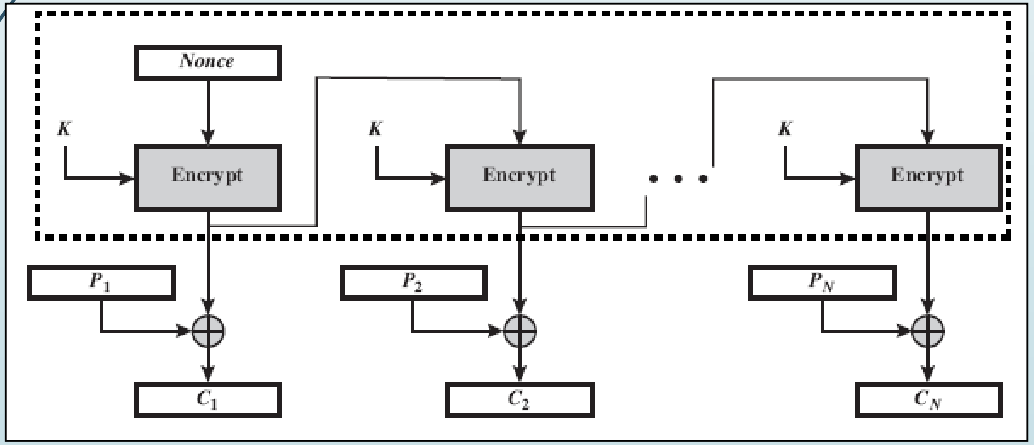
Cipher Feedback (CFB) mode encryption



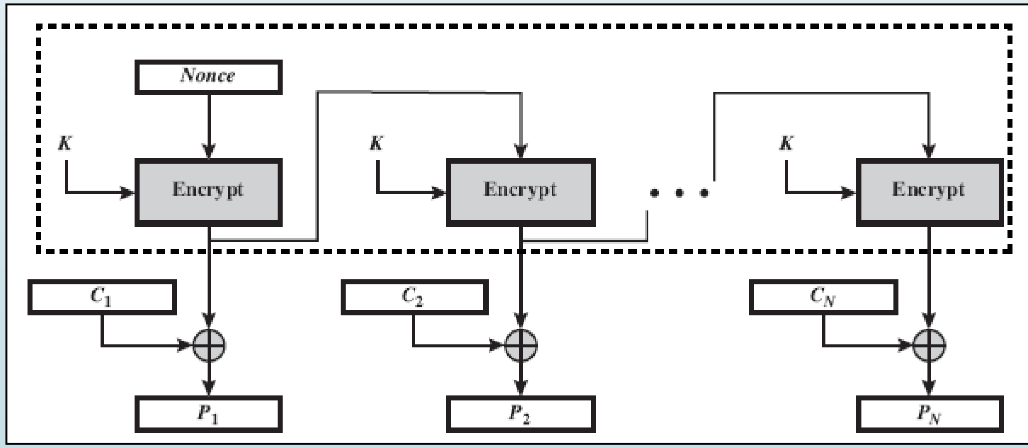
Cipher Feedback (CFB) mode decryption

5) OFB (output feedback) Mode

- ❑ The algorithm create key stream bits that are used for encryption subsequent data blocks.
- ❑ The way of working of the block cipher becomes similar to the way of working of a typical stream cipher.



Encryption



Decryption