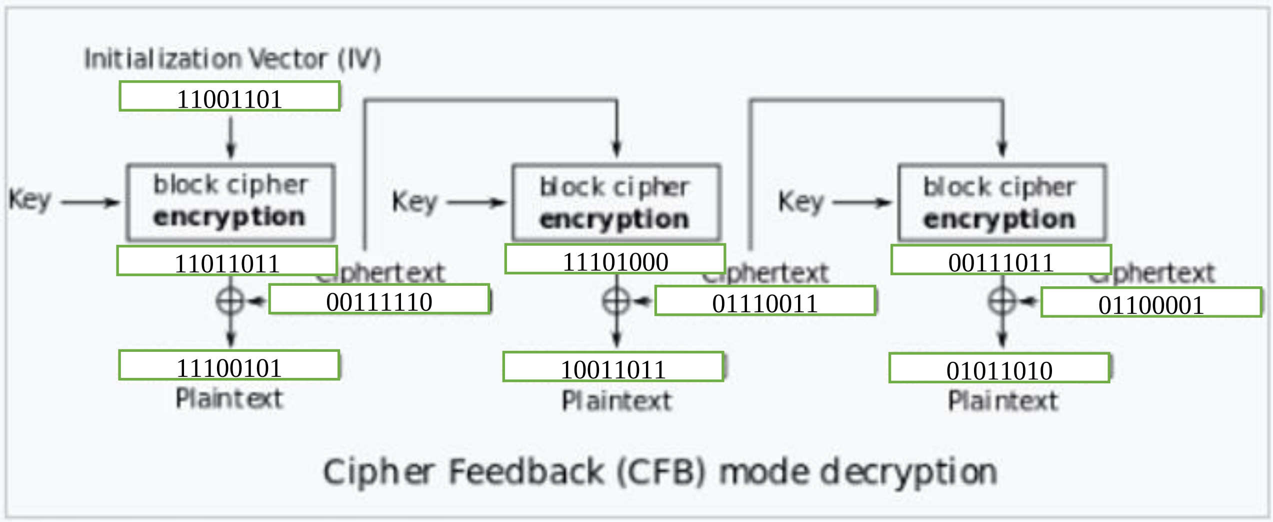
L3 – Computer Systems (2023/2024)

IT Security and Cryptography – Interrogation (Corrected version)

Exercise 01: Full-Block CFB Decryption

We want to decrypt the following bitstream (**001111100111001101100001**) using a full-block CFB mode (**Block size** = **8 bits**). The encryption function is a Feistel Bijection while the random function ***f*** is a simple transposition (**3421**). **IV** = **11001101**

Decryption:



Cipher feedback (CFB) decryption

Step 1: (02 pts)

IV = 11001101

E(IV) = 11011011

+

C1 = 00111110

=

P1 = 11100101

Step 2: (02 pts)

IV = C1 = 00111110 – L+f(D) = 0011+1011 = 1000

E(C1) = 11101000

+

C2 = 01110011

=

P2 = 10011011

Step 3: (02 pts)

IV = C2 = 01110011 – L+f(D) = 0111+1100 = 1011

E(C2) = 00111011

+

C3 = 01100001

=

P3 = 01011010

Plaintext = 11100101.10011011.01011010

Exercise 02: ADFGVX Decryption (Arabic version)

The letters ADFGVX are replaced by the Arabic letters (أ د ف ج ب س). The encryption matrix is filled by the 28 Arabic Alphabet letters (ا ب ت ....و ي) and then the eight digits (١...٨). All the reasoning is done form Right to Left.

- Decrypt the ciphergram " د ف أ أ أ ج ج أ أ س أ ب س د س س د د - - - س ب " knowing that the key is the word طروادة. (the letters أ ، ة could be replaced by ا ، ت).

1) Reorder the columns (letters of the key) according to the Alphabetical order then write the Ciphergram letters row by row: (1.5 pts)

و	ط	ر	د	ة	ا
ج	أ	أ	أ	ف	د
ب	أ	س	أ	أ	ج
د	د	س	س	د	س
	ب	س			

2) Reorder the columns according to the order of letters in the key: (1.5 pts)

ة	**د**	**ا**	**و**	**ر**	**ط**
ف	أ	د	ج	أ	أ
أ	أ	ج	ب	س	أ
د	س	س	د	س	د
				س	ب

3) Read the message row by row: (0.75 pt)

أ أ ج د أ ف أ س ب ج أ أ د س د س س د ب س

4) Construct the encryption matrix: (1.5 pts)

س	**ب**	**ج**	**ف**	**د**	أ	
ح	ج	ث	ت	ب	أ	أ
س	ز	ر	ذ	د	خ	**د**
ع	ظ	ط	ض	ص	ش	**ف**
م	ل	ك	ق	ف	غ	**ج**
٢	١	ي	و	هـ	ن	**ب**
٨	٧	٦	٥	٤	٣	**س**

5) Read the plaintext message (polybe principle) : (0.75 pt)

افتح يا سمسم ٢٤