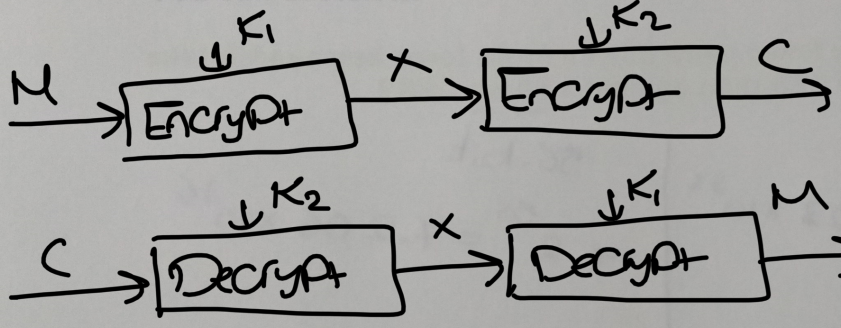
Cairo University
Faculty of Engineering
Computer Engineering Department

جامعة القاهرة
كلية الهندسة
قسم هندسة الحاسبات

Tuesday 21 مارس 2017	تأمين الحاسبات Computer Security	CMP 425 رابعة – هندسة الحاسبات

Answer as much as you can:-
Weight of questions are shown:

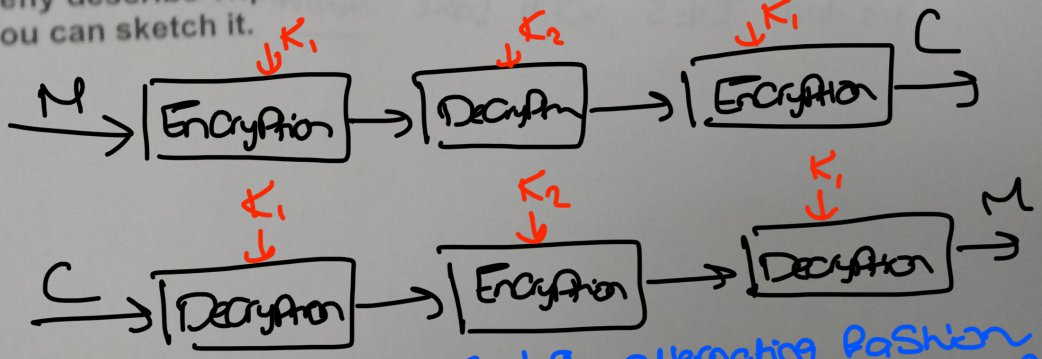
1-a: Briefly describe Double DES With 2 Keys (use only the space below).
You can sketch it.



- It does encryption over two stages with a key for each stage
- This effectively doubles the actual keylength to 112 bits.

I can also write eqns

- Briefly describe Triple DES With 2 Keys (use only the space below).
You can sketch it.



I can write eqns.

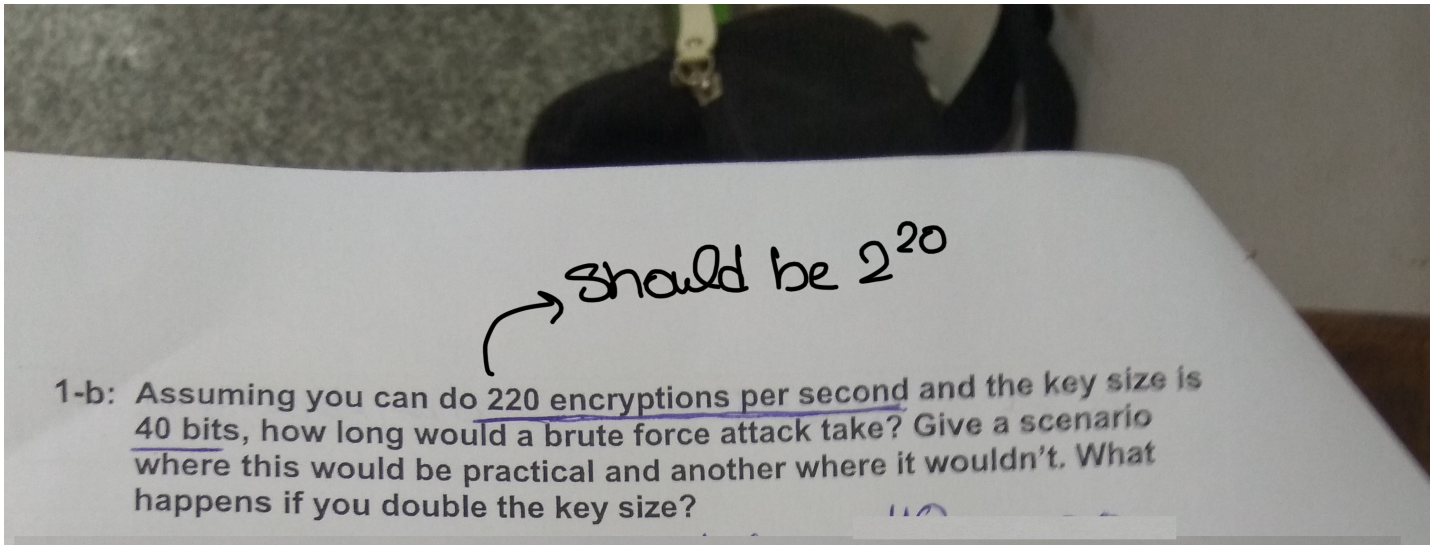
- Two keys are used in alternating fashion
- The fact that middle stage is an decryption → compatibility

- Which one is more secure double DES or triple Des and why:

3DES More secure

WHY: Explain:

It's much more computationally secure than 2DES (resistant to meet in the middle attack) search space is 2^{112}, 2^{56} rather than 2^{56}. 2^{56} (can elaborate further)



→ should be 2^{20}

1-b: Assuming you can do 220 encryptions per second and the key size is 40 bits, how long would a brute force attack take? Give a scenario where this would be practical and another where it wouldn't. What happens if you double the key size?

- 220 encryptions per second
- Key Size = 40 bits → need 2^{40} encryptions

⇒ Exhaustive brute force attack takes

$$\text{time} = \frac{\#\text{encryptions}}{\text{encryptions sec}} = \frac{2^{40}}{2^{20}} \cdot \frac{1}{3600}\,\text{sec} \cdot \frac{1}{24}\,\text{hours} \simeq 12\ \text{days}$$

Whenever useful time of message < 12 days (eg. knowing missile locations on a cold war)

→ Not Practical if say the message to decrypt is about the King being assisinated in 24 hours.

- Doubling Key Size ⇒ time = 2^{40} · 12 days with current computational Power there will never be a scenario where this Practical.

1-c: About how many times more does a brute force key search take against a 112-bit DES than against a 56-bit DES?

- if only ciphertext is known ⇒ $\frac{2^{112}}{2^{56}} = 2^{56}$
- if Plaintext is known (meet-in-the-middle)

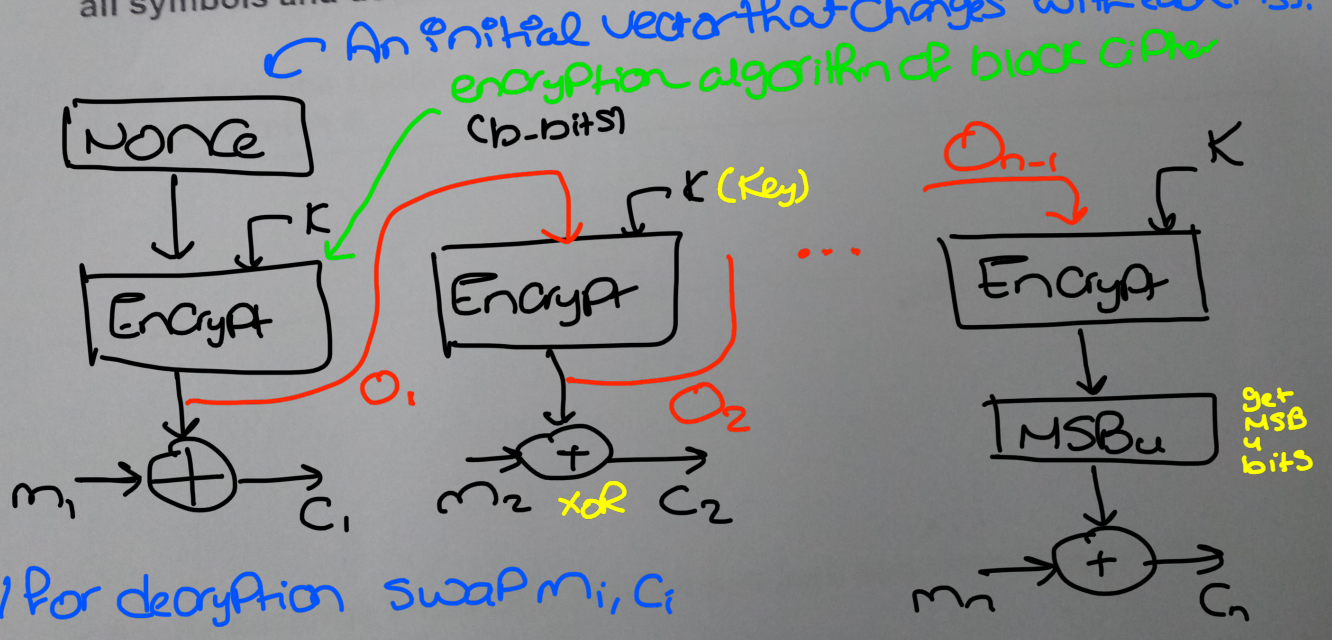
$\frac{2^{56}+2^{56}}{2^{56}} = 2$ (ignoring sort/match time)

2- There are 5 modes of operations of DES Block. One of these modes is Output Feedback (OFB). These modes involve how the different blocks are related together or how feedback is used.

2-a: State the five Cipher Modes of Operation

1. Output feedback OFB.
2. Cipher feed back
3. Counter
4. electronic Code book
5. Cipher block chain

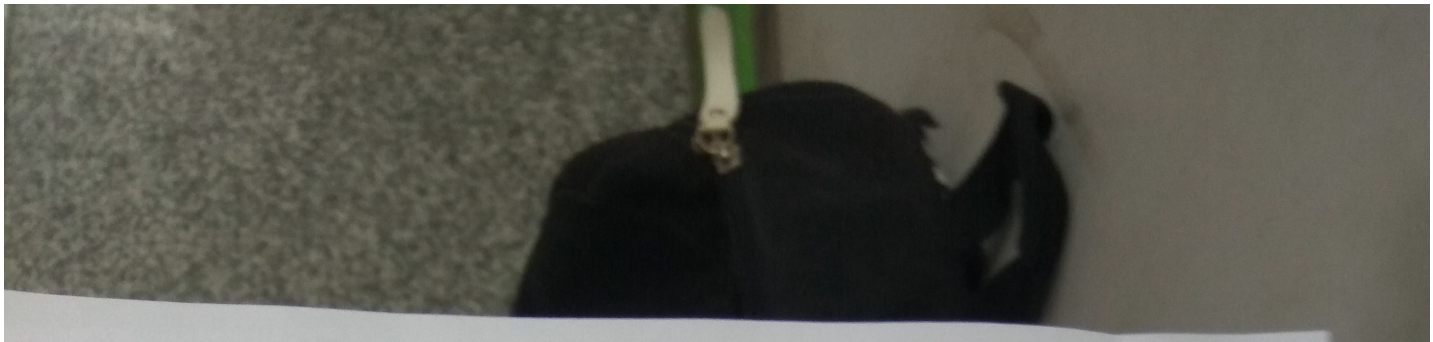
2-b: Draw the block diagram of Out Feedback OFB cipher (SKETCH) show all symbols and details on the sketch.



// For decryption swap m_i, C_i

- Assume message M is Partitioned into $m_1, m_2, \ldots, m_n$ each except for m_n is b bits and m_n is u bits.

// Can write equations



2-c: State and Explain the advantages and Disadvantages of Out Feedback OFB cipher.

Advantages Out Feedback OFB cipher	Disadvantages Out Feedback OFB cipher
• Repetition in msg blocks isn't exposed.	• Vulnerable to message stream modification (mi changed → Ci changed Predictably)
• No need to Pad the message.	• Unlike ECB, neither encryption nor decryption can be Parallelized
• Oi's can be generated before observing msg (Preprocessing)	• Unlike ECB, Counter, random enc./dec. is not Possible (need all Oi's) → Send ≠ receive
• If Ci gets Corrupted in Channel only Mi gets Corrupted. (good for noisy Channel)	• Error in IV affects all Cipher/Plaintext.
• only need to implement the block cipher's encryption block.	• Need to Change IV at both Sender and receiver Foreach message (Synchronising IV)
• Simple Compared to other modes like CFB.	

Crack the Cipher (find a, b)

$$C = aM + b \mod 26$$

- Knowing that

$$M = e_{(4)} \longrightarrow C = b_{(1)}$$ // most freq. letter

$$M = t_{(19)} \longrightarrow C = u_{(20)}$$ // 2nd most freq. letter

$\Rightarrow$ Plugging the first we get:

$$1 = 4a + b \mod 26$$

$\Rightarrow$ Plugging the 2nd we get

$$20 = 19a + b \mod 26$$

$4a + b \equiv 1 \pmod{26}$

$19a + b \equiv 20 \pmod{26}$

Hence (Subtract)

$15a \equiv 19 \pmod{26}$

$\cdot 15^{-1} \equiv 7 \pmod{26}$

Hence $a \equiv 19 \times 7 \pmod{26}$

$a \equiv 3 \pmod{26}$

Thus,

$b \equiv 1 - 4 \times 3 \pmod{26}$

$\equiv 15 \pmod{26}$