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.**

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

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

More secure

WHY: Explain:

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?

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?

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. ....
3. ....
4. ....
5. ....

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

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

Advantages Out Feedback OFB cipher	Disadvantages Out Feedback OFB cipher