Cairo University
Faculty of Engineering
Computer Engineering Department

جامعة القاهرة
كلية الهندسة
قسم هندسة الحاسبات

| 27 May 2015 | تأمين الحاسبات وحالات استشارية<br>Computer Security and Consultations | CMP 425<br>رابعة – هندسة الحاسبات |
|---|---|---|

Answer as much as you can:-
TIME : Part-1 15 Pages 69 Minutes
Part-2 8 Pages 24 Minutes
Use back pages if needed.
All Exam : 23 Pages 120 Minutes

PART-1 Cryptography and Network Security

هذا الجزء مخصص له 96 دقيقة فقط من زمن الامتحان ومخصص له 80% من الدرجة الكلية للتحريرى

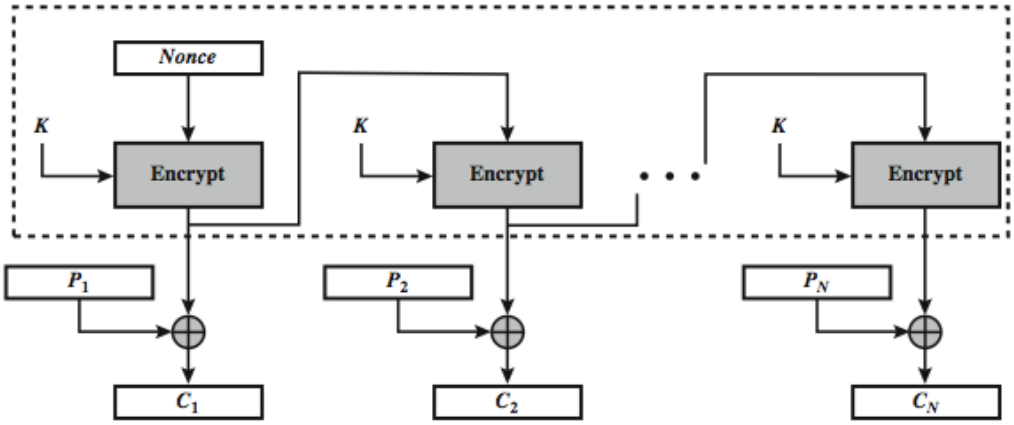
Assume any Missing data and State and Justify your assumptions.

1- 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.

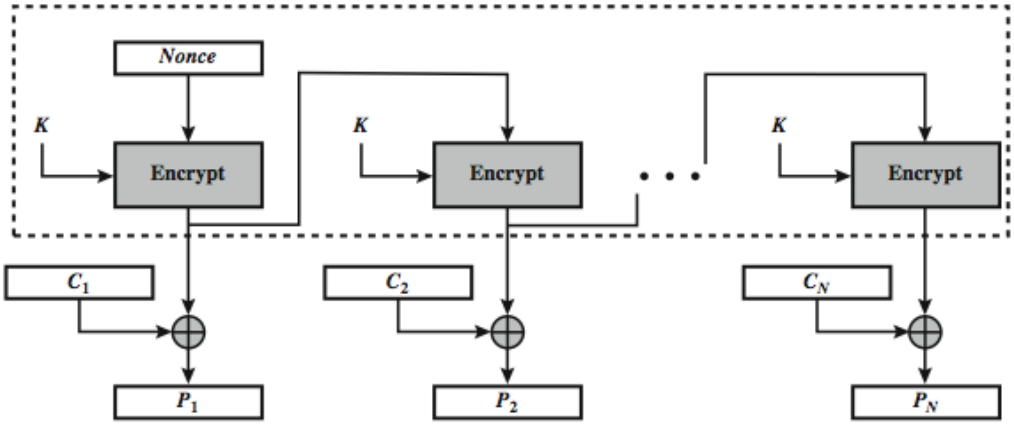
1-a: State the five Cipher Modes of Operation and explain in one line.

1- **Electronic Codebook Book (ECB):** message is broken into independent blocks which are encrypted, encoded independently of the other blocks, $C_i = E_K(P_i)$.
2- **Cipher Block Chaining (CBC):** message is broken into blocks, linked together in encryption operation, each previous cipher blocks is chained with current plaintext block.
3- **Cipher FeedBack (CFB):** message is treated as a stream of bits, added to the output of the block cipher, result is feed back for next stage.
4- **Output FeedBack (OFB):** message is treated as a stream of bits, output of cipher is added to message, output is then feed back.
5- **Counter (CTR):** similar to OFB but encrypts counter value rather than any feedback value.

## 1-b: Draw the block diagram of Out Feedback OFB cipher (SKETCH)




(a) Encryption




(b) Decryption

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

| **Advantages** | **Disadvantages & Limitations** |
|---|---|
| Bit errors do not propagate. | - Needs an IV which is unique for each use<br>  o if ever reuse attacker can recover outputs<br>- More vulnerable to message stream modification.<br>- Sender & receiver must remain in sync.<br>- Only use with full block feedback.<br>  o Subsequent research has shown that only **full block feedback** (ie CFB-64 or CFB-128) should ever be used |

1-d: For each of the modes of operation in the DES protocol named: ECB ,CBC and CTR

- Identify which decrypted blocks Px will be corrupted if there is an error in block C4 of the transmitted cipher text. (Explain).

- **In ECB:** The only corrupted block will be P4, since **ECB** broke messages into independent blocks which are encrypted and encoded independently of other blocks.
- **In CBC:** The corrupted block will be P4 and P5, since **CBC** chains previous cipher blocks with current plaintext block.
- **In CTR:** The only corrupted block is P4, since **CTR** must have a different key & counter value for every plaintext block (never reused).

2-a: Write the Deffie-Hellman Key Exchange technique . Show in detail the details of your derivation and how Diffie-Hellman works.

Global Public Elements

q: prime number

a: a < q and primitive root of q

User A Key Generation

Select private XA , XA < q

Calculate public YA, $YA = a^{YA} \bmod q$

User B Key Generation

Select private XB , XB < q

Calculate public YB, $YB = a^{XB} \bmod q$

Calculation of Secret Key by User A

$K = (YB)^{XA} \bmod q$

Calculation of Secret Key by User B

$K = (YA)^{XB} \bmod q$

The derivation:

$$
\begin{aligned}
K &= (Y_B)^{X_A} \bmod q \\
&= (\alpha^{X_B} \bmod q)^{X_A} \bmod q \\
&= (\alpha^{X_B})^{X_A} \bmod q && \text{by the rules of modular arithmetic} \\
&= \alpha^{X_B X_A} \bmod q \\
&= (\alpha^{X_A})^{X_B} \bmod q \\
&= (\alpha^{X_A} \bmod q)^{X_B} \bmod q \\
&= (Y_A)^{X_B} \bmod q
\end{aligned}
$$

Users A and B use the Diffie-Hellman key exchange technique with a Common prime q = 71 and a primitive root = 7.

- If user A has private key $X_A = 5$, what is A's public key $Y_A$?

$Y_A = 7^5 \ mod \ 71 = 51$

- If user B has private key $X_B = 12$, what is B's public key $Y_B$?

$Y_B = 7^{12} \ mod \ 71 = 4$

- What is the shared secret key?

$K = (YB)^{XA} \bmod q = (YA)^{XB} \bmod q$

Used for subsequent encryption of messages between A and B

2-b: Describe Triple DES with 2 Keys (use only the space below).

It can use 2 keys with E-D-E sequence

- $C = E_{K1}(D_{K2}(E_{K1}(P)))$
- nb encrypt & decrypt equivalent in security
- if K1=K2 then can work with single DES

**2-c: What is the Double DES version of the 56-bit DES with 2 Keys each 56 bits.**

It could use 2 DES encrypts on each block

- $C = E_{K2}(E_{K1}(P))$

**2-d: Explain why Double DES with 2 Keys each 56 bits is much less secure than a single 112-bit DES? (Explain in detail and use sketch when possible).**

Issue of reduction to single stage, and have "meet-in-the-middle" attack:

- since $X = E_{K1}(P) = D_{K2}(C)$
- attack by encrypting P with all keys and store
- then decrypt C with keys and match X value
- can show takes $O(2^{56})$ steps, which is better than exhaustive search at $O(2^{112})$

3-a: You are asked to design a secure hash function. What are the characteristics needed in a secure hash function?

The characteristics of a secure hash function are:

| Requirement | Description |
|---|---|
| Variable input size | H can be applied to a block of data of any size. |
| Fixed output size | H produces a fixed-length output. |
| Efficiency | $H(x)$ is relatively easy to compute for any given $x$, making both hardware and software implementations practical. |
| Preimage resistant (one-way property) | For any given hash value $h$, it is computationally infeasible to find $y$ such that $H(y) = h$. |
| Second preimage resistant (weak collision resistant) | For any given block $x$, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$. |
| Collision resistant (strong collision resistant) | It is computationally infeasible to find any pair $(x, y)$ such that $H(x) = H(y)$. |
| Pseudorandomness | Output of H meets standard tests for pseudorandomness. |

## 3-b: State and describe briefly the phases of operation of a virus or worm.

• **Dormant phase:** The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.

• **Propagation phase:** The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.

• **Triggering phase:** The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.

• **Execution phase:** The function is performed, which may be harmless, e.g. a message on the screen, or damaging, e.g. the destruction of programs and data files

## 3-c: Describe how does a worm propagate

To replicate itself, a network worm uses some sort of network vehicle such as email, remote execution or remote login capabilities. The new copy of the worm program is then run on the remote system where, in addition to any functions that it performs at that system, it continues to spread in the same fashion.

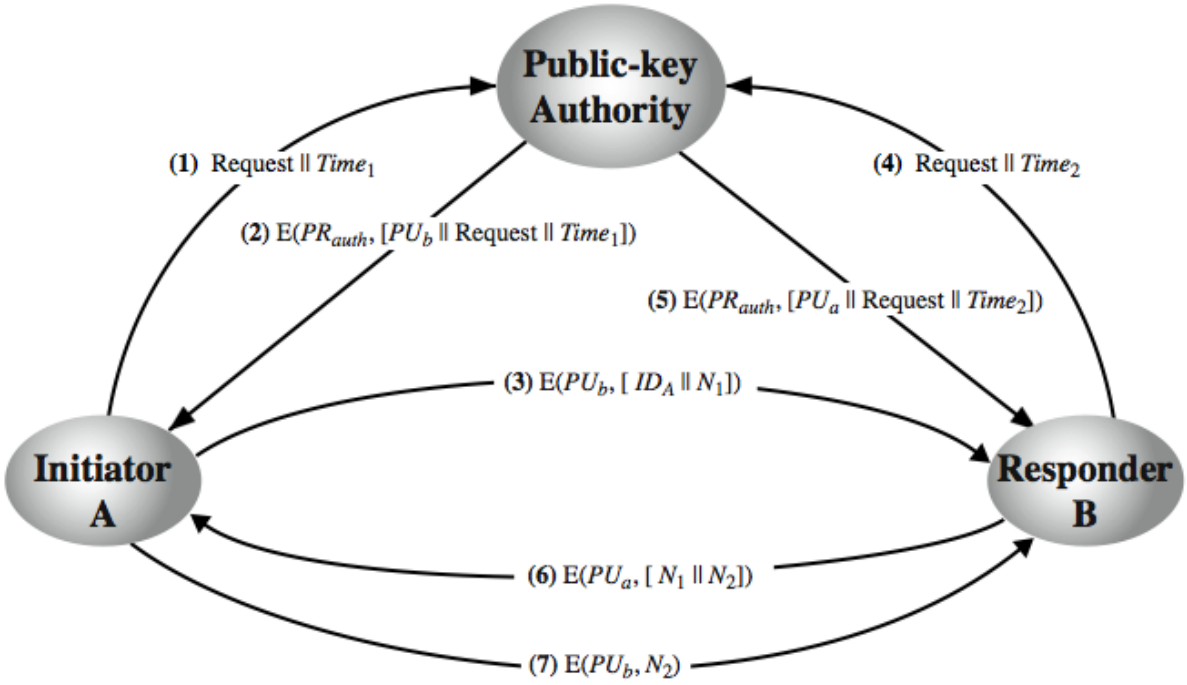
## 3-d: What is a honey pot ?

- It is a decoy systems to lure attackers
    - away from accessing critical systems
    - to collect information of their activities
    - to encourage attacker to stay on system so administrator can respond
- Filled with fabricated information
- Instrumented to collect detailed information on attackers activities
- Single or multiple networked systems

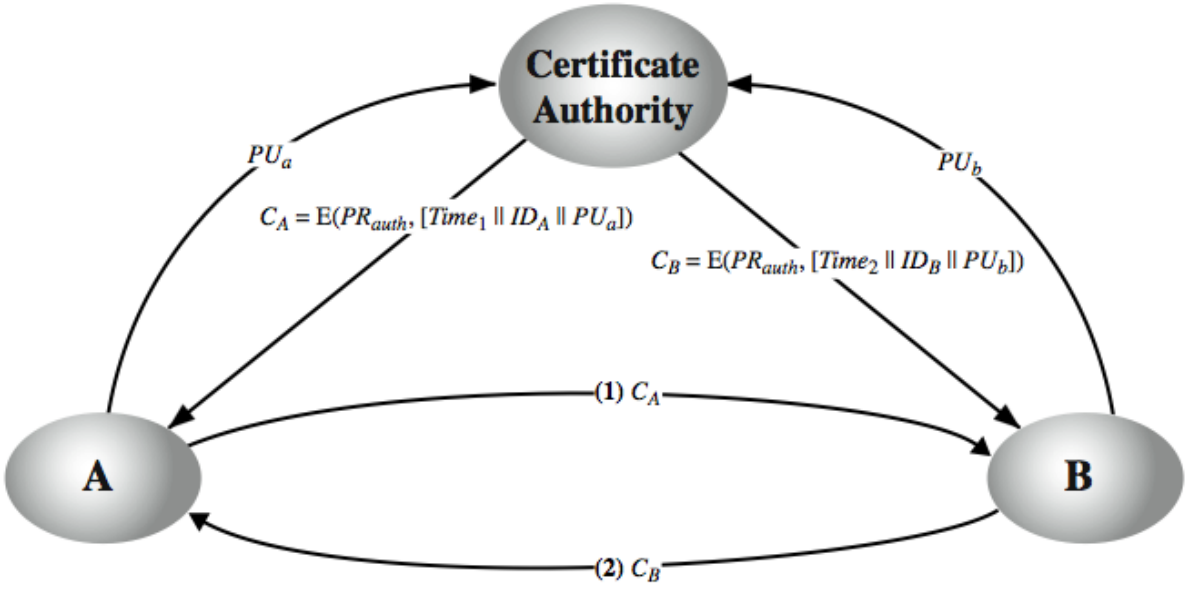
## 3-e: What is the main drawback of the one time pad cryptosystem?

- There is the practical problem of making large quantities of random keys.

4-a: Assume you have a Public Key distribution authority. Sketch the diagram showing how Public key Encryption is used to distribute Secret Keys. [PUT on your sketch all necessary explanation to show how the operation is performed, its order and any necessary explanation].



4-b: Sketch the diagram showing how Certificates are used in a Public Key distribution encryption. [PUT on your sketch all necessary explanation to show how the operation is performed, its order and any necessary explanation].




For participant **A**, the authority provides a certificate **CA** (Certificate Authority or a trusted public key). **A** may then pass this certificate on to any other participant, who can read and verify the certificate by verifying the signature from the certificate authority. Because the certificate is readable only using the authority's public key, this verifies that the certificate came from the certificate authority.

The timestamp serves as something like an expiration date. If a certificate is sufficiently old, it is assumed to be expired.

5-a: Assuming you can do 1 (ONE) encryption 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?

- Number of alternative keys = $2^{40}$, Time required at 1 second = $2^{39}$ second. (*Ch02: Slide 11*).

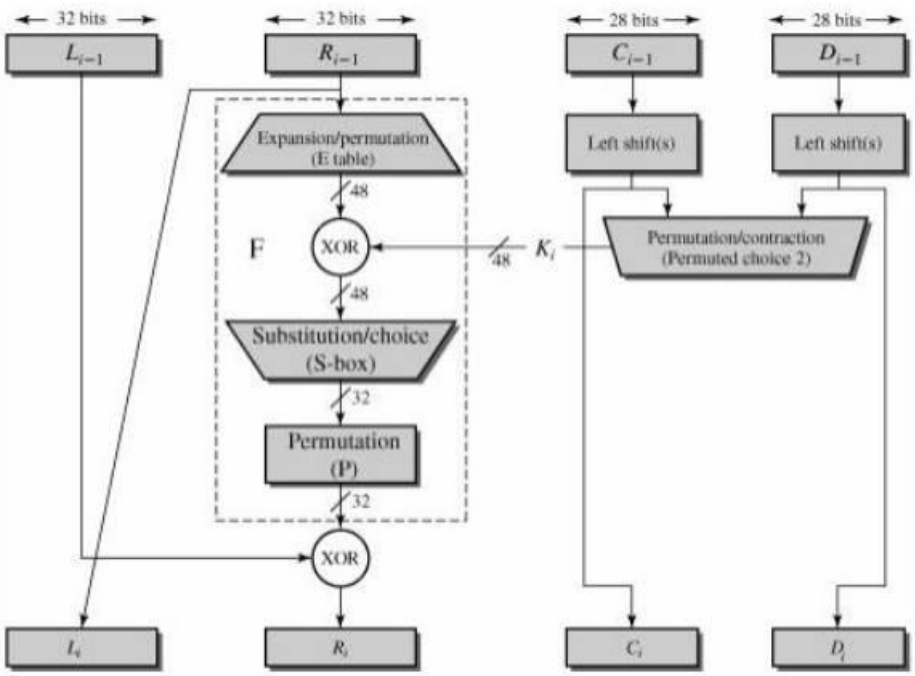
5-b: About how many times more does a brute force key search take against a 112-bit DES than against a 56-bit DES?

$$A\ brute\ force\ against\ a\ 112-bit\ DES\ takes\ \frac{2^{111}}{2^{55}}$$
$$= 2^{56}\ times\ the\ one\ against\ 56-bit\ DES.$$

5-c: What types of attacks are addressed by message authentication? State and describe briefly at least 3 types of attack.

1. Disclosure: Release of message contents to any person or process not possessing the appropriate cryptographic key.
2. Traffic analysis: Discovery of the pattern of traffic between parties. In a connection-oriented application, the frequency and duration of connections could be determined. In either a connection-oriented or connectionless environment, the number and length of messages between parties could be determined.
3. Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or nonreceipt by someone other than the message recipient.
4. Content modification: Changes to the contents of a message, including insertion, deletion, transposition, and modification.
5. Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.
6. Timing modification: Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.
7. Source repudiation: Denial of transmission of message by source.
8. Destination repudiation: Denial of receipt of message by destination.

6-a: Draw, in detail, one round of the DES Algorithm.
[PUT on your sketch all necessary explanation to show how the operation is performed, its order and any necessary explanation].




6-b: Briefly define a group, ring, and field.

- **A group**: a set of elements or "numbers", that may be finite or infinite, with some operation whose result is also in the set (closure).
- **A ring:** a set of "numbers" with two operations (addition and multiplication) which form an abelian group with addition operation and multiplication.
- **A field:** a set of numbers with two operations which form:
    - abelian group for addition,
    - and abelian group for multiplication (ignoring 0),
    - ring

  and have hierarchy with more axioms/laws: group -> ring -> field.

6-c: Use extended Euclidean algorithm to find the multiplicative inverse (if exists) of 826 mod 2789. Show steps in detail.

2789x + 826y = gcd(2789, 826y)

"The Finding Inverses" algorithm:

```
EXTENDED EUCLID(m, b)
1. (A1, A2, A3)=(1, 0, m);
   (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = gcd(m, b); no inverse
3. if B3 = 1
   return B3 = gcd(m, b); B2 = b^-1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 - Q B1, A2 - Q B2, A3 - Q B3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2
```

**Note**: Remember that we calculate T1, T2 and T3 before A1, A2 and A3, so when calculating B1, B2 and B3 we will use the old values of A1, A2 and A3.

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| - | 1 | 0 | 2789 | 0 | 1 | 826 |
| A3/B3=3 | A1=B1=0 | A2=B2=1 | A3=B3=826 | B1=T1,<br>T1=A1-QB1<br>=1-3*0=1<br>B1=1 | B2=T2,<br>T2=A2-QB2<br>=0-3*1=-3<br>B2=-3 | B3=T3,<br>T3=A3-QB3<br>=2789-<br>3*826<br>=311<br>B3=311 |
| 2 | 1 | -3 | 311 | -2 | 7 | 204 |
| 1 | -2 | 7 | 204 | 3 | -10 | 0 |

Since B3=0:
return A3 = gcd(2789, 826); no inverse.