سؤال الاول :

تقدمت شركة لشراء عدد 100 جهاز كمبيوتر ... سعر الجهاز 4500 جنيه

و شراء عدد 100 طابعة ... سعر الواحدة 1950 جنيه

التأمين المقدم مع فتح المظاريف يسمى .....

قمية التأمين المدفوع = ... جنيه

التأمين المقدم بعد ارساء العرض على الشركة يسمى .....

قيمة التأمين المدفوع = ...

السؤال التانى:

اذا تقدمت شركة لمناقصة لتوريد عدد 200 جهاز كمبيوتر لجامعة القاهرة ... و بعد توريد الكمية ارادت جامعة القاهرة زيادة الكمية ل 300 كمبيوتر بدلا من 200 ..... هل تلتزم الشركة بتوريد ال 100 جهاز الزيادة ؟

اشرح الموقف القانونى للشركة ؟

اشرح ما يمكن ان تقوم به جامعة القاهرة فى هذه الحالة ؟

السؤال التالت :

اذا تقدمت شركة لتوريد عدد 200 جهاز كمبيوتر بسعر 4000 للجهاز و كان ميعاد التوريد هو 1 ديسمبر 2011

و تانى افضل عرض فى المتقدمين يورد الجهاز بمبلغ 4500 و اغلى عرض فى المتقدمين يورد الجهاز ب 4800

ماذا يجب على الشركة دفعه للمورد فى الحالات الاتية :

اذا ورد 50 جهاز فى يوم 28 نوفمبر 2011

اذا ورد 50 جهاز فى يوم 1 ديسمبر 2011

اذا ورد 50 جهاز فى يوم 15 يناير 2011

اذا امتنع المورد عن توريد اخر 50 جهاز فى ال 200 جهاز المتفق عليهم

اشرح الموقف القانونى للجهة الادارية بالنسبة للمورد فى حالة الامتناع عن اداء القيمة الباقية من التوريد ؟

اذكر محتويات المظروف الفنى بطريقتك مع ترتيبهم من حيث الاولوية الاهم فالمهم ؟

نصف الدرجة على الترتيب الصحيح من حيث الاهمية ؟

كيف يتم دفع التأمين ؟

متى يتم الغاء المناقصة او المزايدة ؟ اشرح كل نقطة

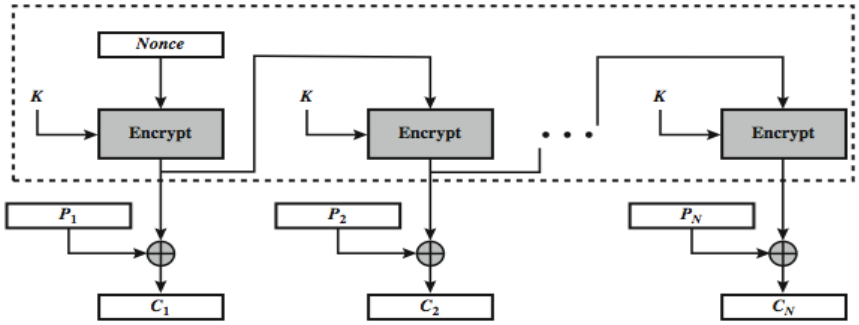
فى رأيك لماذا يكون هناك مظروفين مختلفين .. احدهما فنى و الاخر مالى و لا يجب فتح المظروف المالى الا بعد ان يتم قبول العرض فنيا ؟

ما هى شروط الاعلان عن المناقصة و ماذا يجب ان يتوفر فى الاعلان ؟

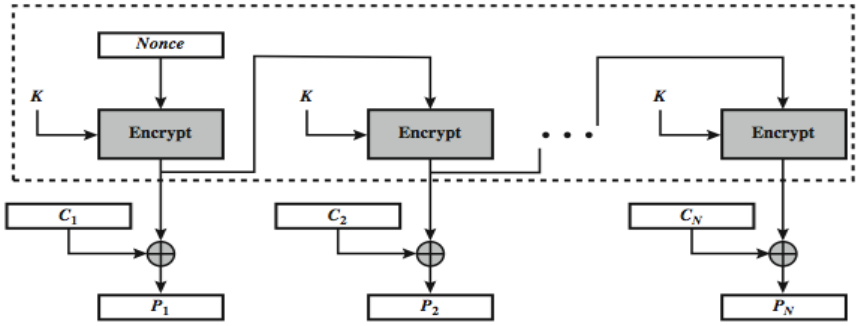
-Mention the Five modes of operation of Block Cipher?

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key or IV)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed s bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	• Stream-oriented transmission over noisy channel (e.g. satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

-Sketch the Output Feed Back Mode diagram and write the necessary equations for encryption and decryption?



(a) Encryption



(b) Decryption

$O_i = E_K(O_{i-1})$

$C_i = P_i$ XOR O_i

$O_{-1} = IV$

-Compare between OFB Advantages and Disadvantages?

- needs an IV which is unique for each use
  - if ever reuse attacker can recover outputs
- bit errors do not propagate
- more vulnerable to message stream modification
- sender & receiver must remain in sync
- only use with full block feedback
  - subsequent research has shown that only **full block feedback** (ie CFB-64 or CFB-128) should ever be used

- Write Equation of Diffie Hellman Algorithm and solve the following question ?

Given Q, A, XA calculate YA?

Given Q, A, XB calculate YB?

Calculate the shared Key KAB?

2. (Final 2010) Two users are using Diffe-Hellman with alpha = 7 and q = 71. If Xa = 5, compute Ya. If Xb = 12, compute Yb. Compute the secret key. (this question is identical to problem 10.1 in the book)

Sol:

$Y_A = \alpha^{XA} \bmod q = 51$

$Y_B = \alpha^{XB} \bmod q = 4$

$K = (Y_B)^{XA} \bmod q = K = (Y_A)^{XB} \bmod q = 30$

-What is the shared Secret Key?

It is the key used by sender and receiver to encrypt and decrypt the messages, it is only known to both of them only

-what are the characteristics needed in secure hash function?

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* ! *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

-Mention 3 objective of the HMAC Design?

- use, without modifications, hash functions
- allow for easy replaceability of embedded hash function
- preserve original performance of hash function without significant degradation
    - Use and handle keys in a simple way.
- have well understood cryptographic analysis of authentication mechanism strength

- To use, without modifications, available hash functions. In particular, hash functions that perform well in software, and for which code is freely and widely available.
- To allow for easy replaceability of the embedded hash function in case faster or more secure hash functions are found or required.
- To preserve the original performance of the hash function without incurring a significant degradation.
- To use and handle keys in a simple way.
- To have a well understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions about the embedded hash function.

-what types of attack are addressed by message authentication?

1. **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.
2. **Content modification:** Changes to the contents of a message, including insertion, deletion, transposition, and modification.
3. **Sequence modification:** Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.
4. **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.

-Draw Needham Schroeder Protocol (KDC) , write equation and specify all the details of it ?

- If we tried to use the Needham Schroeder Protocol in the E-mail Application what the modifications to be done on it?

-Identify Classes of intruders?

1. **Masquerader**: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.
2. **Misfeasor**: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.
3. **Clandestine user**: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

-what the common two technique to protect password file?

1. **One-way encryption:** The system stores only an encrypted form of the user's password. When the user presents a password, the system encrypts that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the encryption function and in which a fixed-length output is produced.
2. **Access control:** Access to the password file is limited to one or a very few accounts

-in intruder detection, what is the difference between statistical anomaly and rule based detection?

1. **Statistical anomaly detection** involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.
2. **Rule-Based Detection** involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder

-what is HoneyPot?

Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.

What is a salt in UNIX Password management and why is it used?

The salt is combined with the password at the input to the one-way encryption routine.

-List 4 techniques to avoid guessable password?

1. **User education:** Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords.
2. **Computer-generated passwords:** Users are provided passwords generated by a computer algorithm.
3. **Reactive password checking:** the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed and notifies the user.
4. **Proactive password checking:** a user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it.

-list and describe the 4 phases of operation of virus and worms?

• **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

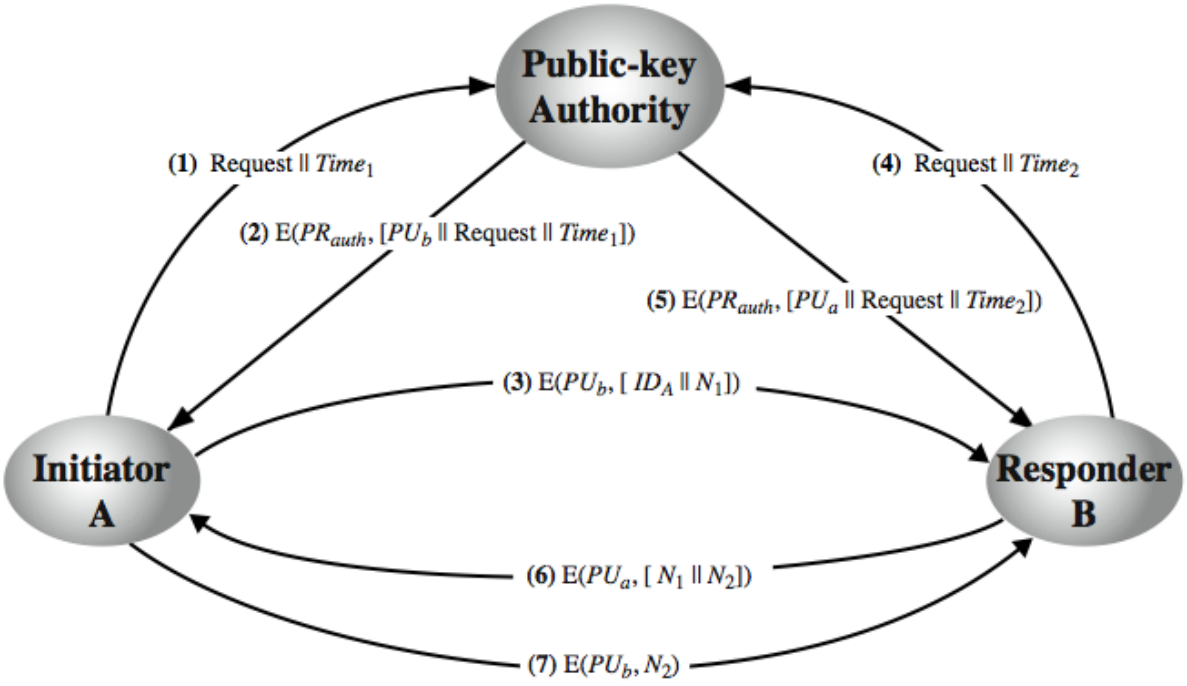
-describe how does the worm propagate?

1. Search for other systems to infect by examining host tables or similar repositories of remote system addresses.
2. Establish a connection with a remote system.
3. Copy itself to the remote system and cause the copy to be

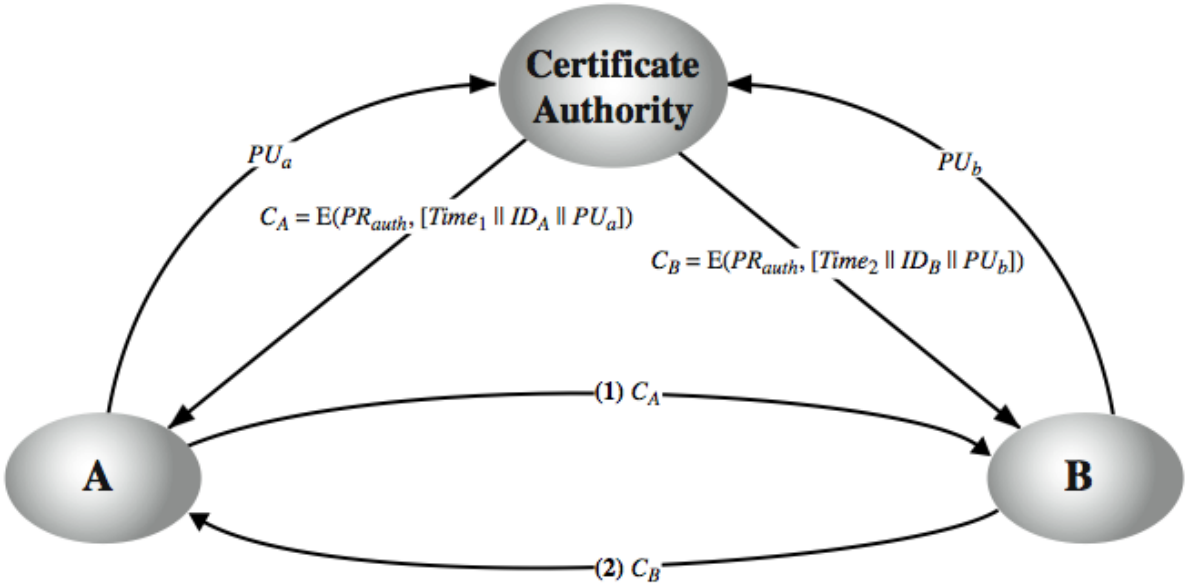
-what is the disadvantage of the one pad time cryptosystem?

1. Key generation
2. key distribution

-Draw Authority Key Distribution mechanism and illustrate all the equation needed?



--Draw Certificate Key Distribution mechanism and illustrate all the equation needed?



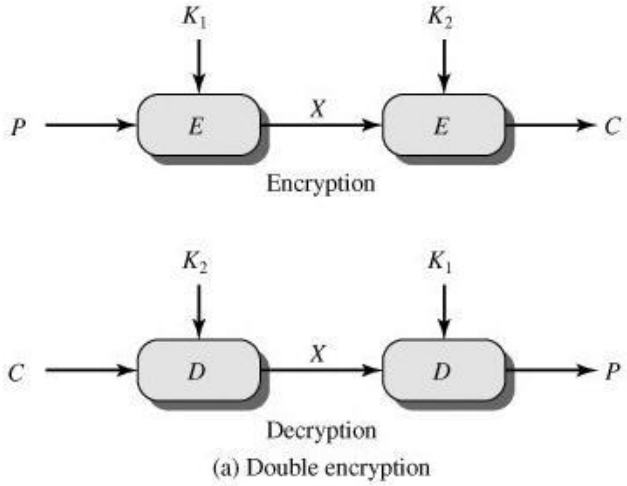
If RSA Algorithm were used and Bob and Alice where exchanging message, Bob leaks his Private key , and as a solution he decide to generate a new public and private key ?

Is that safe?

-Illustrate your answer?

Explain the Double DES and Triple DES and write the needed Equation for them? Draw the block diagram of both?

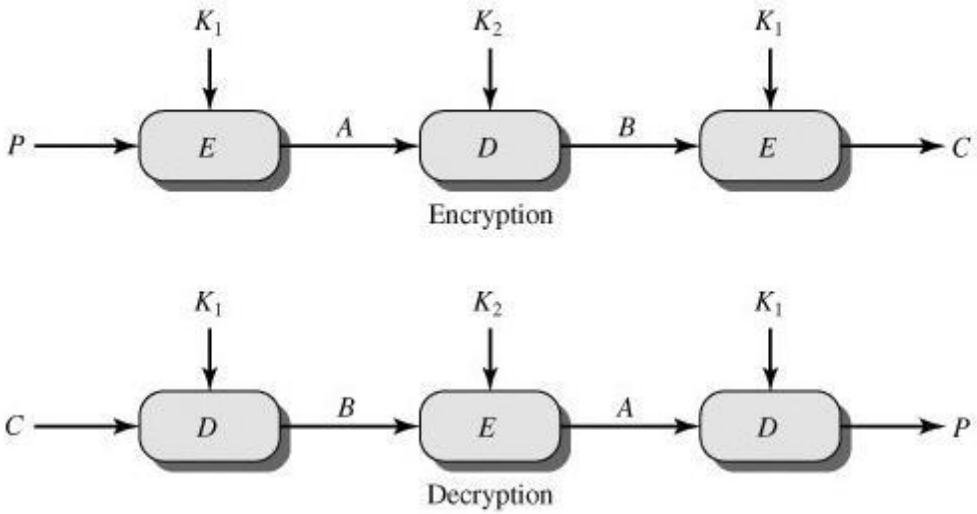
Double DES



(a) Double encryption

Encryption: $C = E(K_2, E(K_1, P))$.
- **Decryption:** $P= D(K_2, D(K_1, P))$.

Triple DES



$C = E(K_1, D(K_2, E(K_1, P)))$

Why Double Des with two keys each one with size of 56 bits is less secure than Des with one Key with size of 112 bits?

Meet-in-the-Middle Attack

$C = E(K_2, E(K_1, P))$
$X = E(K_1, P) = D(K_2, P)$
Given a known pair, (P, C)
1. Encrypt P for all 2_{56} possible values of K_1 Store these results in a table and then sort the table by the values of X.
2. Decrypt C using all 2_{56} possible values of K_2. As each decryption is produced, check the result against the table for a match.
3. If a match occurs test the two resulting keys against a new known plaintext-ciphertext pair.
4. If the two keys produce the correct ciphertext, accept them as the correct keys.

Compute the GCD of the Two Following Polynomial?

1. x^4+x^3+x and x^2+1 over GF(2)
2. $2x^3+x^2+2$ and x^2+x+1 over GF(3)

- See section 2 page 8
- Same as figure but replace numbers with polynomials

Ex

- gcd(55, 22) = gcd(22, 55 mod 22) = gcd(22, 11) = 11
- gcd(11, 10) = gcd(10, 1) = gcd(1, 0) = 1

Steps for getting EUCLID(a, b)

1. A ← a; B ← b
2. **if** B = 0 **return** A = gcd(a, b)
   - لو ال B طلعت ب0 يبقى Aهى الgcd بتاعة a&b وأطلع من البرنامج
3. R = A mod B
   - هجيب A mod B وأحطه فى R
4. A ← B
5. B ← R
   - أحط Bمكان A وR مكان B
6. **goto** 2
   - أرجع لخطوة أتنين

Ex

To find gcd(1970, 1066)

1970	= 1 x 1066 + 904	gcd(1066, 904)
1066	= 1 x 904 + 162	gcd(904, 162)
904	= 5 x 162 + 94	gcd(162, 94)
162	= 1 x 94 + 68	gcd(94, 68)
94	= 1 x 68 + 26	gcd(68, 26)
68	= 2 x 26 + 16	gcd(26, 16)
26	= 1 x 16 + 10	gcd(16, 10)
16	= 1 x 10 + 6	gcd(10, 6)
10	= 1 x 6 + 4	gcd(6, 4)
6	= 1 x 4 + 2	gcd(4, 2)
4	= 2 x 2 + 0	gcd(2, 0)

Therefore, gcd(1970, 1066) = 2

Compute the Multiplicative inverse of the following F(x) and G(x) in module GF(2^8)

$x^5+x^4+x^2+1$ in GF (2^8) with m(x)= $x^8+x^4+x^3+x+1$

same as figure but replace A3 and B3 with both polynomials

- 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- QB1, A2-QB2, A3-QB3)
6. (A1, A2, A3) = (B1, B2, B3)
7. (B1, B2, B3) = (T1, T2, T3)
8. **goto** 2

EX: Finding the inverse of 550 in GF(1759)

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	−3	109
5	1	−3	109	−5	16	5
21	−5	16	5	106	−339	4
1	106	−339	4	−111	355	1