

Q1 Solve any two.

- a) Explain with example different approaches to implement security model. 5
1. No Security
  2. Security Through obscurity
  3. Host security
  4. Network Security
- b) Encrypt the message 'Come Home Tomorrow' using 5
- i. Ceaser Cipher
  - ii. Simple Columnar Transposition Techniques with four columns. Order is 3,2,4,1
- i. frph krph wrpruurz  
ii. mmmoooooreeowCHTr
- c) Explain how attackers misuse cookies to collect important information. 5
1. An advertising agency (My Ads) contacts major Web sites and places banner ads for its corporate clients' products on their pages. It pays some fees to the site owners for this.
  2. Instead of providing an actual image that can be embedded by the respective website in their pages directly, it provides a link (URL) to add each page.
  3. Each URL contains a unique number in the file part.
  4. When a user visits a page for the first time, the browser fetches the advertisement image from My Ads along with the main HTML page for the site it is visiting.
  5. When the user visits the main site, My Ads sends a cookie to the browser containing a unique user id and records the relationship between this user id and the file name.
  6. Latter, when the same user visits another page, the browser sees another reference to My Ads.
  7. The browser sends the previous cookie to My Ads and also fetches the current page from My Ads as before.
  8. My Ads knows that the same user has visited another webpage now.
  9. It adds this reference to its database.
- d) List possibilities of attacks when the sender of message encrypts the plain text message into its corresponding cipher text. 5
1. Cipher text only attack
  2. Known plain text attack
  3. Chosen plain text attack
  4. Chosen cipher text attack
  5. Chosen text attack

Q2 Solve any two.

- a) List different cryptography algorithm types. Explain with example. 5
- Stream cipher  
Block cipher
- b) Explain the steps in various rounds of AES. 5
- Apply S-box to each plain text  
Rotate Row k of the plain text block (i.e. state ) by k bytes  
Perform a mix column operation  
XOR the state with key block

c) Explain subkey generation process of blowfish algorithm. 5

There are

32 bit keys generated as  $K_1, K_2, \dots, K_n$

32 bit 18 P-arrays

Four S-boxes each containing 256 32 bit entries

$S_{1,0}, S_{1,1}, \dots, S_{1,255}$

$S_{2,0}, S_{2,1}, \dots, S_{2,255}$

$S_{3,0}, S_{3,1}, \dots, S_{3,255}$

$S_{4,0}, S_{4,1}, \dots, S_{4,255}$

Sub key generation

1. initialize P-array

2. Do bitwise XOR of P! with  $K_1$ , P2 with  $K_2$  until P18. This works until P14 and  $K_{14}$ . For P15 to P18 reuse  $K_1$  to  $K_4$

$P_1 = P_1 \text{ XOR } K_1$

$P_2 = P_2 \text{ XOR } K_2$

$P_3 = P_3 \text{ XOR } K_3$

$P_4 = P_4 \text{ XOR } K_4$

.

.

.

$P_{14} = P_{14} \text{ XOR } K_{14}$

$P_{15} = P_{15} \text{ XOR } K_1$

$P_{16} = P_{16} \text{ XOR } K_2$

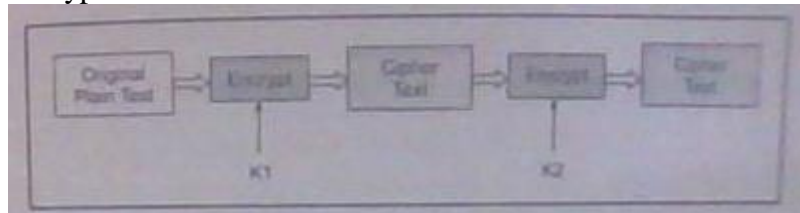
$P_{17} = P_{17} \text{ XOR } K_3$

$P_{18} = P_{18} \text{ XOR } K_4$

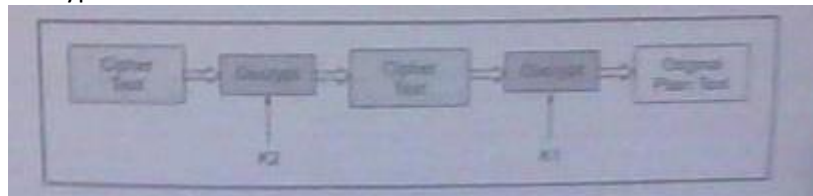
Take a 64 bit block with all 64 bits initialized to 0. Use the above P-array and S-boxes above to run the Blowfish encryption process.

d) Explain double DES algorithm. 5

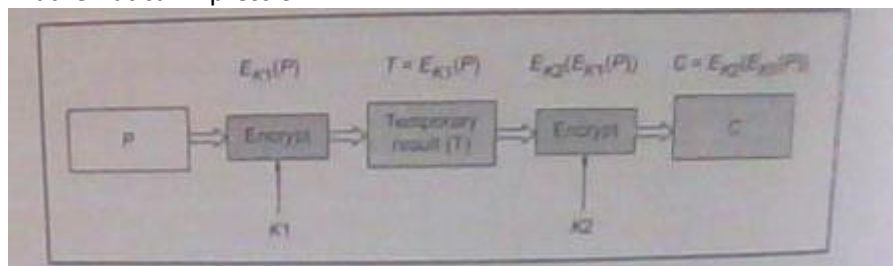
encryption



Decryption



Mathematical Expression



Q3 Solve any two.

- a) Explain how RSA is used for performing digital signature. 5  
Assume A wants to send a message M to B along with the digital signature S calculated over message M.  
Step 1. The sender (A) uses the SHA-1 message digest algorithm to calculate the message digest (MD1) over the original message (M).  
Step 2. The sender (A) now encrypts the message digests with her private key. The output of this process is called as the digital signature (DS).  
Step 3. Now the sender (A) sends the original message (M) along with the digital signature (DS) to the receiver (B).  
Step 4. After the receiver (B) receives the original message (M) and the sender (A's) digital signature, B use the same message digest algorithm as was used by the a and calculate its own message digest (MD2)  
Step 5. The receiver (B) now uses the sender's (A's) public key to decrypt the digital signature.  
Step 6. B now compare two message digests MD1 and MD2.  
If  $MD1 = MD2$   
B accepts the original message (M) as the correct, unaltered message from A  
B is also assured that the message came from A and not from someone posing as A.

- b) Explain how secure hash algorithm -512 works. 5  
Step 2.  
Steps  
Padding  
Append length  
Divide the input into 1024 bit blocks  
Initialize chaining variables  
Process blocks

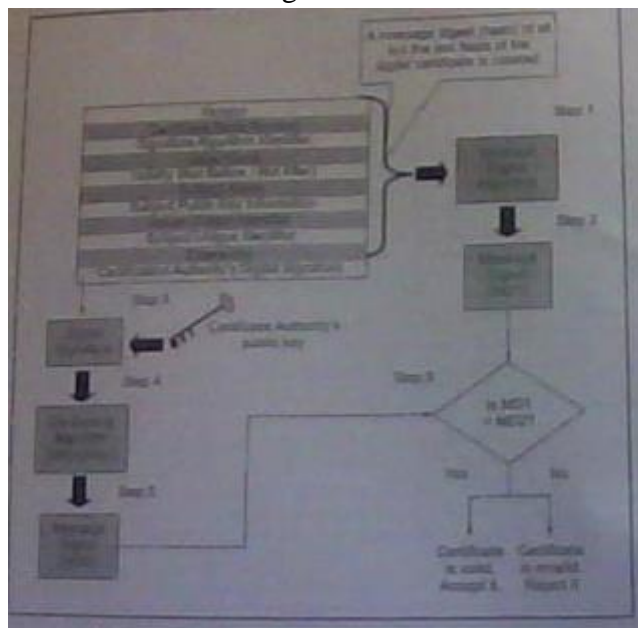
- c) Explain the working of HMAC. 5  
Let  
MD = message digest  
M = input message  
L = number of blocks in the message  
b = number of bits in each blocks  
K = shared symmetric key  
ipad = A string 00110110 repeated b/8 times  
opad = A string 01011010 repeated b/8 times  
Steps  
1. Make the length  $K = b$   
2. XOR K with ipad to produce S1  
3. Append M to S1  
4. Message Digest algorithm  
5. XOR K with opad to produce S2  
6. Append H to S2  
7. Message Digest algorithm

- d) Explain Elipitic Curve Cryptography and EIGamal. 5  
 Introduction  
 Difference between RSA and ECC  
 Explanation of Elliptic curve

Q4 Solve any two.

- a) Describe of the various fields of x.509V3 digital certificate 5  
 various fields of x.509V3 digital certificate are:  
 Authority Key Identifier  
 Subject Key Identifier  
 Key usage  
 Extended Key usage  
 Private Key usage Period  
 Certificate Policies  
 Policy Mappings  
 Subject Alternative Name  
 Issuer Alternative Name  
 Subject Directory Attributes  
 Basic Constraints  
 Name Constraints  
 Policy Constraints

- b) How digital certificate is verified? 5  
 The verification of digital certificate consist of following steps:



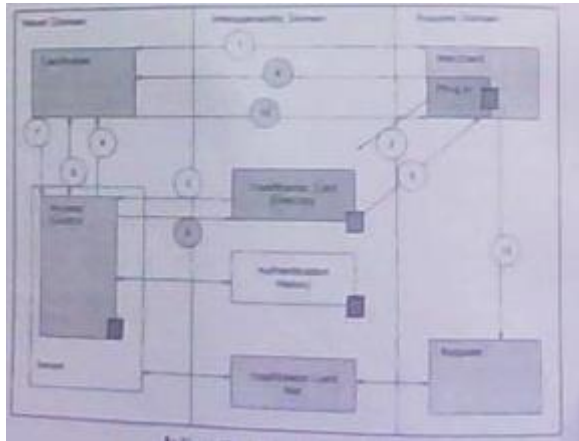
- c) Why do we trust digital certificate. 5  
 d) List and explain public key cryptography standards. 5

Explanation of any five of the following public key cryptography standards:

- PKCS#1 RSA Encryption Standard
- PKCS#2 RSA Encryption Standard for Message Digest
- PKCS#3 Diffie-Hellman Key Agreement Standard
- PKCS#5 Password Based Encryption
- PKCS#6 Extended Certificate Syntax Standard
- PKCS#7 Cryptographic Message Syntax Standard
- PKCS#8 Private Key Information Standard
- PKCS#9 Selected Attribute Types
- PKCS#10 Certificate Request Syntax Standard
- PKCS#11 Cryptographic Token Interface Standard
- PKCS#12 Personal Information Exchange Syntax Standard
- PKCS#13 Elliptic Curve Cryptography Standard
- PKCS#14 Pseudo-Random Number Generation Standard
- PKCS#15 Cryptographic token Information Syntax

Q5 Solve any two.

- a) Explain handshake protocol. 5  
The Handshake protocol is the first sub protocol used by the client and the server to communicate using an SSL-enabled connection.  
Format of handshake protocol.  
Phase 1 : Establish Security Capabilities  
Phase 2 :Server authentication and key exchange  
Phase 3 : Client authentication and key exchange  
Phase 4 :Finish
- b) Explain the Secure Electronic Transaction process. 5  
SET Process
1. The customer opens an account
  2. The customer receives a certificate
  3. The merchant receives a certificate
  4. The customer places an order
  5. The merchant is verified
  6. The order and payment detail are sent
  7. The merchant requests payment authorization
  8. The payment gateway authorizes the payment
  9. The merchant confirms the order
  10. The merchant provides goods or services
  11. The merchant requests payment
- c) With neat diagram write internal operations of 3-D secure protocol. 5  
Explanation



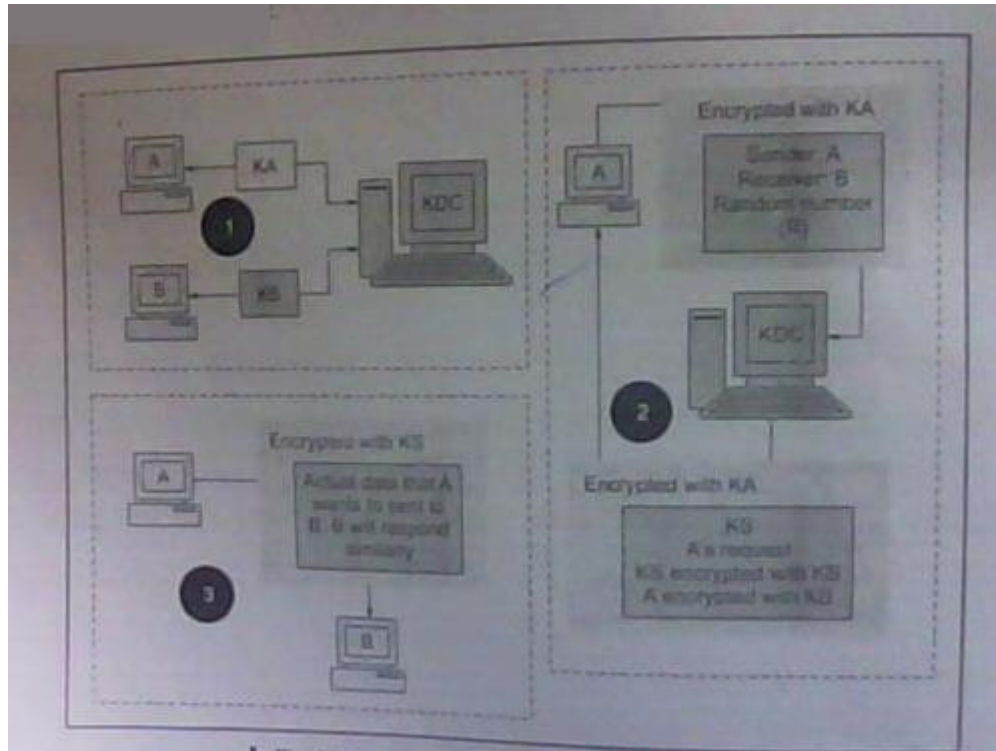
- d) List different firewall configurations. Explain any two. 5
- Different firewall configurations are
1. Screened Host Firewall, Single Homed Bastion
  2. Screened Host Firewall, Dual Homed Bastion
  3. Screened Subnet Firewall
- Explanation of any two.

Q6 Solve any two.

- a) Explain how clear text password works. What are the problems with it? 5
- Every user in a system is assigned with a user id and an initial password which is alterable by the user. The password is stored in the user database against the user id on the server. The authentication mechanism works as
1. Prompt for user id and password
  2. User enters user id and password
  3. user id and password validation
  4. Authentication result
  5. Inform user accordingly.

Problems:

1. Database contains passwords in clear text
  2. Password travels in clear text from the user's computer to the server.
- b) Write a short note on key distribution center. 4
- KDC is central authority dealing with keys for individual computers in computer network. It is similar to the concept of the Authentication Server (AS) and Ticket Granting Server in Kerberos. Every node store unique secrete key with the KDC. Whenever user A wants to communicate securely with user B the following happens:
1. The background is that A has a shared secrete key  $K_A$  with KDC. Similarly B is assume to share a secrete key  $K_B$  with the KDC.
  2. A sends request to KDC encrypted with  $K_A$  which includes
    - a. Identities of A and B.
    - b. A random number R called nonce.
  3. KDC responds with message encrypted with  $K_A$ , containing
    - a. One-time symmetric key  $K_S$
    - b. Original request that was sent by A, for verification.
    - c.  $K_S$  encrypted with  $K_B$  and id of A encrypted with  $K_B$ .
  4. A and B now communicate by using  $K_S$  for encryption



1

c) Explain how challenge/response tokens works. 5

1. User sends a login request
2. Server creates random challenge
3. User signs the random challenge with the message digest for the password.
4. Server verifies the encrypted random challenge received from the user.
5. Server returns on an appropriate message back to the user.

d) What are the One-way authentication approaches? Explain any two. 5

Listing

Explanation

1. Login Only
2. Shared Secrete
3. One-way public key

Q7 Solve any three.

a) Write short note on phishing. 5

Attacker set up a fake web sites, which look like the real website.

The attacker modus operandi works as follows:

1. The attacker decides to create his/her own web site, which looks very identical to a real website.
2. The attacker can use many technique to attack the bank's customer.
3. When the customer clicks on the URL specified in the email (received from attacker) , he/she is taken to the attacker's site and not the original site. There the customer is prompted to enter confidential information . the attacker accepts this information and display thank you message. The attacker now uses the confidential information .

b) Explain subkey generation process of each round of international data 5

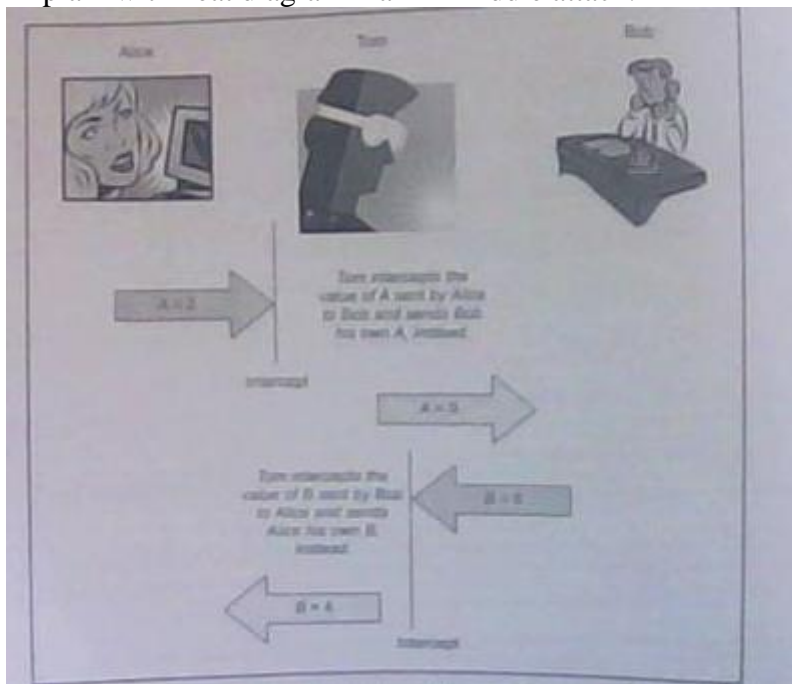
5

encryption algorithm.

Round	Details of the sub-key generation and use
1	Bit positions 1-96 of the initial 128-bit key would be used. This would give us 6 sub-keys K1 to K6 for Round 1. Key bits 97 to 128 are available for the next round.
2	Key bits 97 to 128 make up sub-keys K1 and K2 for this round. A 25-bit shift on the original key happens, as explained. Post this shifting, the first 64 bits are used as sub-keys K3 to K6 for this round. This leaves bits 65 to 128 unused for the next round.
3	Unused key bits 65 to 128 are used as sub-keys K1 to K4 of this round. Upon key evaluation, another 25-bit shift happens, and bits 1 to 32 of the shifted key are used as sub-keys K5 and K6. This leaves bits 33 to 128 unused for the next round.
4	Bits 33 to 128 are used for this round, which is perfectly adequate. No bits are unused at this stage. After this, the current key is again shifted.
5	This is similar to Round 1. Bit positions 1-96 of the current 128-bit key would be used. This would give us 6 sub-keys K1 to K6 for Round 1. Key bits 97 to 128 are available for the next round.
6	Key bits 97 to 128 make up sub-keys K1 and K2 for this round. A 25-bit shift on the original key happens, as explained. Post this shifting, the first 64 bits are used as sub-keys K3 to K6 for this round. This leaves bits 65 to 128 unused for the next round.
7	Unused key bits 65 to 128 are used as sub-keys K1 to K4 of this round. Upon key evaluation, another 25-bit shift happens, and bits 1 to 32 of the shifted key are used as sub-keys K5 and K6. This leaves bits 33 to 128 unused for the next round.
8	Bits 33 to 128 are used for this round, which is perfectly adequate. No bits are unused at this stage. After this, the current key is again shifted for the <i>Output Transformation</i> round.

c) Explain with neat diagram man-in-middle attack.

5



d) Why is a self-signed certificate needed?

5

The certificate authority hierarchy begins with the root CA. The root CA has one or more second level CAs below. Each of these second level CAs can have one or more third level CAs, which in turn have lower level CAs and so on. This hierarchy relieves the root CA from having to manage all the possible digital certificates. Instead the root CA can delegate this job to the second level CA. Each of this second level CA could appoint third level CA and so on.

In this there may be problem of the verification of root CA .

As the root CA is the last in the validation chain, there is no way to validate it's certificate. The root CA and many times, even the second or third level



CAs are automatically considered as trusted CAs. These CAs certificate is a self signed certificate ie the root CA signs its own certificate.

- e) Explain how pretty good privacy works. 5
  - 1. Digital signature
  - 2. Compression
  - 3. Encryption
  - 4. Digital enveloping
  - 5. Base-64 Encoding
- f) How does certificate-based authentication works? 5
  - 1. Creation, Storage and distribution of digital certificate
  - 2. Login request
  - 3. Server creates a random challenge
  - 4. User signs the random challenge
  - 5. Server returns an appropriate message back to the user.