Chapter 1

1. (2015)(mid 2014)(Final 2016) What is meant by computer security? What are goals of computer security?

2. (2013+2015+2014+2019) What is the differences between **active** and **passive** security attacks. Give example for each type that clarifies that difference.

   (OR) (Final 2016) What is meant by network security? List and briefly define categories of passive and active security attacks. [2 marks]

3. (2013) Describe different security attacks. Briefly describe a security measure to prevent these attacks.

4. (2013) For a user workstation in a typical business environment, list potential locations for confidentiality attacks.

5. (2013+2014+2015+2019) (Old Quiz) What is meant by security services? Describe the role of the following security services:
   1. Authentication.
   2. Access Control
   3. Data confidentiality.
   4. Data integrity.
   5. Nonrepudiation.

   Show what security mechanisms can be used for each one of them.

6. (OR) (Final 2016) Introduce different security services that achieve goals of network security and introduce its corresponding different security mechanisms [4 marks]

7. (2014+2015) What is the difference between security services and security mechanisms? Choose three different security services and its corresponding security mechanisms used. Give reasons for its usage.

	Release of message contents	**Traffic analysis**	**Masquerade**	**Replay**	**Modification of messages**	**Denial of service**
Encipherment	**Y**					
Digital signature			**Y**	**Y**	**Y**	
Access control	**Y**	**Y**	**Y**	**Y**		**Y**
Data integrity				**Y**	**Y**	
Authentication exchange	**Y**		**Y**	**Y**		**Y**
Traffic padding		**Y**				
Routing control	**Y**	**Y**				**Y**
Notarization			**Y**	**Y**	**Y**	

Co

8. (Old Mid) For an online company works as a stock Market provider dealer, give examples to its probable security attacks violations and discuss what services could be used to counter these attacks. discuss its corresponding security mechanisms used and why.

	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			**Y**			
Data origin authentication			**Y**			
Access control			**Y**			
Confidentiality	**Y**					
Traffic flow confidentiality		**Y**				
Data integrity				**Y**	**Y**	
Non-repudiation			**Y**			
Availability						**Y**

9. (2019) Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement.

10. (mid 2014) Consider a computer switching network that routes data through a switching network based on the IP number requested by the client. Give examples of confidentiality, and integrity requirements associated with the system and, in each case, indicate the degree of importance of the requirement. Show the required mechanisms that can be used to achieve these services.

11. (2014+2015) Consider a telephone switching system that routes calls through a switching network based on the telephone number requested by the caller. Give examples of confidentiality, and integrity requirements associated with the system and, in each case, indicate the degree of importance of the requirement.

Chapter 2

1. (2014+2015) For a cipher text, when you can say it is computationally secure, and when you can say it is unconditionally secure?

2. (2013+2015) (Old Mid) (Final 2016) Why do some block cipher modes of operation only use encryption while others use both encryption and decryption? Give Examples.

3. (2013+2019) What is the difference between block cipher and stream cipher? (OR) What is the advantage of stream cipher over block cipher techniques?

4. (2013)(Final 2016) List important design considerations for a stream cipher.

12. (Old mid) Encrypt the message "We have been discovered save yourself".
    a) Using a play fair cipher technique with key word "commander".
    b) Using a polyalphabetic technique with key word "Individual".
    c) Using a transposition technique with key "5427136".

Caesar and Mono alphabetic

5. (2015) Discuss what makes Mono alphabetic cipher better than Caesar cipher.
6. (2015) Encrypt the message "Meeting has been postponed until tomorrow morning" using a Caesar cipher and **Monoalphabetic** cipher techniques. **Use a proper key** for each case. Clarify the differences between these two techniques.

Caesar and polyalphabetic

7. (Final 2016) Encrypt the message "**meeting has been changed to be at eight o'clock pm tomorrow"** using:
    a) Caesar cipher
    b) Poly alphabetic cipher technique with the keyword **Convention**.
    c) Clarify the differences between these two techniques. [4 marks].

Play Fair

8. (2013+2014+2015+2019)(Final 2016) Use a play fair method and perform the following:
    a) Construct a play fair matrix using the key word "CIPHER".
    b) How many possible keys does the play fair cipher have? Ignore the fact that some keys might produce identical encryption results. Express your answer as an approximate power of 2.
    c) Encrypt this message: "Meeting has been postponed until tomorrow morning at ten am"
    d) Decrypt this message: "UHSPMNIFCBSCQTHFNHHUEKLCKBIC".
    e) Discuss the disadvantages of using this method and how to improve it.
    f) Discuss the advance of the Playfair cipher over simple monoalphabetic cipher.

9. (2014+2015) Use a Play fair encryption technique do the following:
    a) Construct the play fair matrix using the key word" **UNITED".**
    b) How many possible keys does this cipher have?
    c) Encrypt this message "meet me at the usual place at ten rather than eight oclock".
    d) Decrypt the received message "NXTKKCUEMNSTCXEUJW".

10. (2019) Use a play fair method with key word "common", encrypt the message" public must help to secure country against terror attacks ".

Vigenère cipher

11. (2013) This problem explores the use of a **one-time** pad version of the **Vigenère cipher**. In this scheme, the key is random numbers between 0 and 26. For example, if the key is 3 19 5 …, then the first letter of plaintext is encrypted with a shift of three letters, the second with a shift of 19 letters, the third with a shift with 5 letters, and so on.
    a) Encrypt the plaintext sendmoremoney with the key stream 9 0 1 7 23 15 21 14 11 11 2 8 9.
    b) Using the ciphertext produced in part (a), find a key so that the cipher text decrypts to the plaintext cashnotneeded.

One-time pad

12. (2014+2015)(Final 2016) Why One-Time pad security is unbreakable? Discuss the advantages amd problems of using this technique [2 marks]

2) (Mid 2014) Discuss the One-Time pad cipher security.

Rail-fence & Row Transposition (transposition techniques)

1. (2013) You have been given the following message:
   "TOTINXBWSLNAOLIYDANOMTAAPIOBCNDKEMPIAINNOLURCARXIIDHUEAZ"
   You know by somehow that the original message has been encrypted using a transposition technique with key length 7. Decrypt this message and find its original message.

2. (2014+2015) Show how you can apply a transposition ciphering technique to the following message "we have been discovered save yourself" using the key "3 2 4 1 5". What is your opinion about this ciphering technique? Discuss how you can improve such technique.

1. (Mid 2014) You received this message "PDOWOZHOSULTOEDIMLIOTRECIPRWTDTKEYECNNECXNUGEBNM". You know that the technique used to decrypt this message is a transposition one but you lost the key, decrypt it and deduce its key.

3. (2014+2015) You and your brother agreed to send important messages through a communication network using a transposition encryption technique. The key you will go to use is "4 7 3 5 2 6 1". Do the following:
    a) Encrypt this message "I will deposit a twenty thousand dollars in your bank account. Please send me your account number".
    b) Decrypt your brother replied message: "UEEONNBZCMIEVTLXANSRSGAKMNRTUEAACUFEEHHWOBVFEIYYYTIHRILN".
    c) Discuss **advantages** and **disadvantages (weaknesses)** of using this technique. **What modifications** you can do **to improve** this technique.
    d) Compare between this technique and play fair technique method from point of view of cryptanalysis.

Chapter 3

1. (2013+2015) Discuss the difference between **diffusion and confusion**? Why is it important to consider these notions in designing a block cipher algorithms?

2. (Mid 2014) Discuss the concept that the modern encryption cipher technique is based on and show using figure(s) how it is applied in a simple D.E.S.

2. (2014+2015) What is the purpose of the S-boxes and P-boxes in DES?

3. (2014+2015) Using a simplified DES. Encrypt the following string: 11010111
   use the key: 0110111001.

   P10: 3 5 2 7 4 10 1 9 8 6; P8: 6 3 7 4 8 5 10 9

   IP: 2 6 3 1 4 8 5 7; IP^{-1}: 4 1 3 5 7 2 8 6

   E/P: 4 1 2 3 2 3 4 1 P4: 2 3 4 1

S0	0	1	2	3
0	1	0	3	2
1	3	2	0	1
2	0	2	1	3
3	3	1	3	2

S1	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

4. (2015) (Mid 2014) Using a simplified DES approach do the followings:
   a) Draw a simplified DES algorithm.
   b) Decrypt the following string: **10100010**. Show all steps required. Use the following parameters:

   The key: 0111111101.

   P10: 3 5 2 7 4 10 1 9 8 6; P8: 6 3 7 4 8 5 10 9

   IP: 2 6 3 1 4 8 5 7; IP^{-1}: 4 1 3 5 7 2 8 6

   E/P: 4 1 2 3 2 3 4 1; P4: 2 3 4 1

S_0:	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S_1	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

5. (2019) Using S-DES, Decrypt the string (10101110) using the key (0110011101) by hand. Show S-DES diagram and intermediate steps after each function. Use the following parameters:

   P10: 3 5 2 7 4 10 1 9 8 6; P8: 6 3 7 4 8 5 10 9

   IP: 2 6 3 1 4 8 5 7; IP^{-1}: 4 1 3 5 7 2 8 6

   E/P: 4 1 2 3 2 3 4 1; P4: 2 3 4 1

S_0:	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S_1	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

6. (2019) (Final 2016) Using S-DES, Encrypt the string (10100011) using the key (1110011011) by hand. Show S-DES diagram and intermediate steps after each function. Use the following parameters:

P10: 3 5 2 7 4 10 1 9 8 6; P8: 6 3 7 4 8 5 10 9

IP: 2 6 3 1 4 8 5 7; IP^{-1}: 4 1 3 5 7 2 8 6

E/P: 4 1 2 3 2 3 4 1; P4: 2 3 4 1

S_0:	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S_1	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

Unknown

SSL

3. (2019) Describe using suitable figure phases of SSL handshake protocol.

PGP

4. (2015) Why does **PGP** generate a signature before applying compression?

5. (2015) Describe briefly the five principal services provided by **PGP**.

6. (2019) Discuss process of PGP mail security and illustrate using figures how transmission and reception process. Why does PGP generate a signature before applying compression?

7. (2015) PGP makes use of the cipher feedback (CFB) mode of CAST-128, whereas most symmetric encryption applications (other than key encryption) use the cipher block chaining (CBC) mode. We have
   CBC: Ci = E(K, [Ci-1 _ Pi]); Pi = Ci-1 _ D(K, Ci)
   CFB: Ci = Pi_ E(K, Ci-1); Pi = Ci_ E(K, Ci-1)
   These two appear to provide equal security. Suggest a reason why PGP uses the CFB mode.

MAC & Hash Code

8. (2013) What is the difference between a MAC and a hash code?

9. (2013) Show by diagram the usage of MAC code (C) for message authentication and confidentiality, where authenticator tied to plain text.

10. (2015) Discuss two different applications of the Cipher Hash Function and illustrate, using figures, how it is done in each case.

11. (Using a suitable figure) (2013) Using of a hash code to provide message authentication in case of confidentiality as well as a digital signature is desired.

Virus types

12. (2013) List and briefly describe five categories among the most significant types of viruses.

13. (2013) Discuss the similarities and differences between virus and worm from the point of view:
    - Type of attack.
    - Operation.

Kerberos

14. (2019) (using suitable figure) In a distributed environment, discuss approaches used to secure authentication. What are the principal differences between version 4 and version 5 of Kerberos?

15. (using a suitable figure) (2013) What four requirements were defined for Kerberos? What entities constitute a full-service Kerberos environment?

16. (2015) Discuss the following:
    a) The problem was Kerberos designed to address.
    b) Entities constitute a full-service Kerberos environment.
    c) The principal differences between version 4 and version 5 of Kerberos.

17. (2015+2019) You want to build a hardware device to do block encryption in the cipher block chaining (CBC) mode using an algorithm stronger than DES. 3DES is a good candidate. Design two different possibilities, one loop CBC and three loops as another one, both of which follow from the definition of CBC. Which of the two would you choose: (مش شرط الرسمة تيجي)
    1. For security?
    2. For performance?

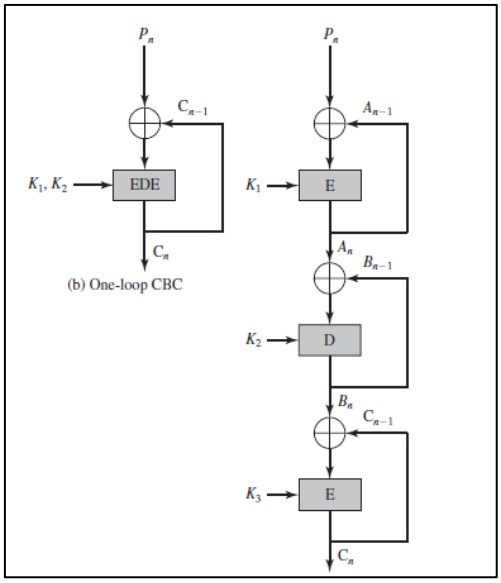


Figure 1. one Loop and Three Loop CBC mode.

RC4

18. (2019) For a given plain text "10101010 11001101", apply a stream cipher technique RC4 to find its cipher text, use 4 bytes states and 2 bits key K[ ] = [3, 5]. Discuss its relative advantages to block cipher one.

Public Key (RSA)

19. (2019) Perform encryption and decryption using the RSA algorithm for p = 11, q = 13, e =11; M = 7.

20. (2015) In a public-key using RSA, you intercept the cipher text C = 57 sent to a user whose public key is e = 17, n = 77, deduce the plaintext M.

21. (2019) While you are using the public-key system using RSA, you intercept the cipher text C = 10 sent to a user whose public key is e = 5, n = 35, deduce the plaintext M.

22. (2013) Perform encryption and decryption using the RSA algorithm for p = 11, q = 13, e =11; M = 7. While you are using the public-key system using RSA, you intercept the cipher text C = 10 sent to a user whose public key is e = 5, n = 35, deduce the plaintext M.

23. (2013+2015) What requirements must a public key cryptosystem fulfill to be a secure algorithm?

24. (2013) Illustrate by suitable figure how we can use public key cryptosystem in secrecy and authentication in the same time?

25. (2013) What is a public key certificate?

26. (2013) Given the two primes P & Q equals to 47 & 71 respectively, generate a public key pair and use it to encrypt the value 688, Verify?

27. (using a suitable figure) (2013) What are some approaches to produce message authentication? Give an example for each approach; use a suitable figure to illustrate how each of them is used for message authentication.

28. (2019) Describe approaches used to produce message authentication. Give an example for each approach; use a suitable figure to illustrate how each of them is used for message authentication.

29. Describe three groups of functions used to produce an authenticator. Show by diagram the three usages of public-Key encryption for confidentiality, authentication and digital signature.

30. (2013) List and briefly define three classes of intruders. What are three benefits that can be provided by an intrusion detection system (or) what corresponding intruder detection system that can efficiently detect them.

31. (2015) Discuss how honey pot and password are used in protection against intruders.

Revision Sheet

a) You work as an IT security manager for a company. Its computers, workstations and servers are connected through internet. Highlight different security attacks that could confront its computers, workstations, and servers. Justify security services and corresponding mechanisms that can be used to overcome these attacks.

Answer:

security attacks

- **Interruption:** This is an attack on availability
  - Disrupting traffic
  - Physically breaking communication line
- **Interception:** This is an attack on confidentiality
  - Overhearing, eavesdropping over a communication line
- **Modification:** This is an attack on integrity
  - Corrupting transmitted data or tampering with it before it reaches its destination
- **Fabrication:** This is an attack on authenticity
  - Faking data as if it were created by a legitimate and authentic party

---

- A **security service** is a measure to address a threat
  - E.g. authenticate individuals to prevent unauthorized access
- A **security mechanism** is a means to provide a service
  - E.g. encryption, cryptographic protocols
- A security service is a service provided by the protocol layer of a communicating system (X.800)
- 5 Categories
  - Authentication: Ensuring the proper identification of entities and origins of data before communication
  - Access Control: Preventing unauthorized access to system resources
  - Data confidentiality: Preventing disclosure to unauthorized parties
  - Data Integrity: Preventing corruption of data
  - Nonrepudiation (and Availability): Collecting proof to prevent denial of participation in transaction or communication. Availability Protection against denial-of-service.

Security Mechanisms

- Two types
  - Specific mechanisms existing to provide certain security services
    - E.g. encryption used for authentication
  - Pervasive mechanisms which are general mechanisms incorporated into the system and not specific to a service
    - E.g. security audit trail

b) Explain the essential ingredients of a symmetric encryption. Justify to what extent symmetric encryption algorithms satisfy Shannon prospective for strong encryption algorithm?

Answer:

- **Plain Text:** original data or input
- **Encryption Algorithm:** performs substitutions or transformations on the plaintext
- **Public and Private Keys-** also input determines the substitutions/transpositions
- **Cipher Text-** scrambled message or output
- **Decryption Algorithm-** encryption algorithm run backward, taking the cipher text and producing the plain text**.**

c) Justify why of the middle portion of 3 DES is a decryption rather than an encryption?

Answer:

There is no cryptographic significance to the use of decryption for the second stage. Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES by repeating the key.

d) Differentiate between Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes of operations from the point of view of its operation and applications used.

Answer:

Electronic Codebook Book (ECB):

- message is broken into independent blocks which are encrypted

- each block is a value which is substituted, like a codebook, hence name
- each block is encoded independently of the other blocks

  $C_i = DES_{K1}(P_i)$

- uses: secure transmission of single values

Cipher Block Chaining (CBC):

- message is broken into blocks
- linked together in encryption operation
- each previous cipher blocks is chained with current plaintext block, hence name
- use Initial Vector (IV) to start process

  $C_i = DES_{K1}(P_i \text{ XOR } C_{i-1})$
  $C_{-1} = IV$

- uses: bulk data encryption, authentication

e) Some block cipher modes of operation only use encryption while others use both encryption and decryption. Discuss why this is the case in the context of operation and application used.

Answer:

- Some modes of operation (e.g. CTR) work in such a way that only known values are ever encrypted, forming a stream of pseudo-random data that is then combined with the plaintext by a keyless reversible operation (often xor) to form the ciphertext.
- Other modes (e.g. CBC) directly encrypt secret (i.e. plaintext) values, meaning decryption is required to find out what the secret value was.
- One of the biggest advantages of a scheme that does not require decryption is that it can be implemented in hardware with reduced footprint (i.e. it's smaller). Moreover, for block ciphers such as AES it can often be easier to implement efficient encryption than decryption because the internal coefficients have been optimized for this direction.
- Some modes of operation only use an encryption function because it is used to generate something to XOR with the plaintext. There is no point decrypt the generated bytes. To decrypt the ciphertext, you just need the same stream of bytes.

f) For a given plain text “10111010 10111101”, apply a stream cipher technique RC4 to find its cipher text, use 4 bytes states and 2 bits key K[ ] = [3, 5]. Discuss its relative advantages to block cipher one.

Answer:

iteration 1:

i = 0 , f = 0 , g = 0

S[] = [S0, S1, S2, S3] = [0, 1, 2, 3]

K[] = [K0, K1] = [3, 5]

Because f = (f + S0 + K0) mod 4 = (0 + 0 + 3) mod 4 = 3

Then swap S0 with S3

New array S[] = [S0, S1, S2, S3] = [3, 1, 2, 0]

i = i + 1 = 1

g = (g + 1) mod 2 = 1

iteration 2:

i = 1 , f = 3 , g = 1

S[] = [S0, S1, S2, S3] = [3, 1, 2, 0]

K[] = [K0, K1] = [3, 5]

Because f = (f + S1 + K1) mod 4 = (3 + 1 + 5) mod 4 = 1

Then swap S1 with S1

New array S[] = [S0, S1, S2, S3] = [3, 1, 2, 0]

i = i + 1 = 2

g = (g + 1) mod 2 = 0

iteration 3:

i = 2 , g = 0 , f = 1

S[] = [S0, S1, S2, S3] = [3, 1, 2, 0]

K[] = [K0, K1] = [3, 5]

Because f = (f + S2 + K0) mod 4 = (1 + 2 + 3) mod 4 = 2

Then swap S2 with S2

New array S[] = [S0, S1, S2, S3] = [3, 1, 2, 0]

i = i + 1 = 3

g = (g + 1) mod 2 = 1

iteration 4:

i = 3 , g = 1 , f = 2

S[] = [S0, S1, S2, S3] = [3, 1, 2, 0]

K[] = [3, 5]

because f = (f + S3 + K1) mod 4 = (2 + 0 + 5) mod 4 = 3

Swap S3 with S3

New array S[] = [S0, S1, S2, S3] = [3, 1, 2, 0]

This example we use Plaintext "1011 1010 1011 1101"

i = 0 , f = 0

S[] = [S0, S1, S2, S3] = [3, 1, 2, 0]

Because i = (i + 1) mod 4 = 1

f = (f + S1) mod 4 = 1 Then swap S1 with S1

New array S[] = [S0, S1, S2, S3] = [3, 1, 2, 0]

t = (S1 + S1) mod 4 = 2

S2 = 2 (0000 0010)

```
  1011 1010
XOR 0000 0010
-------------
  1011 1000
```

for "1011 1101"

i = 1 , f = 1

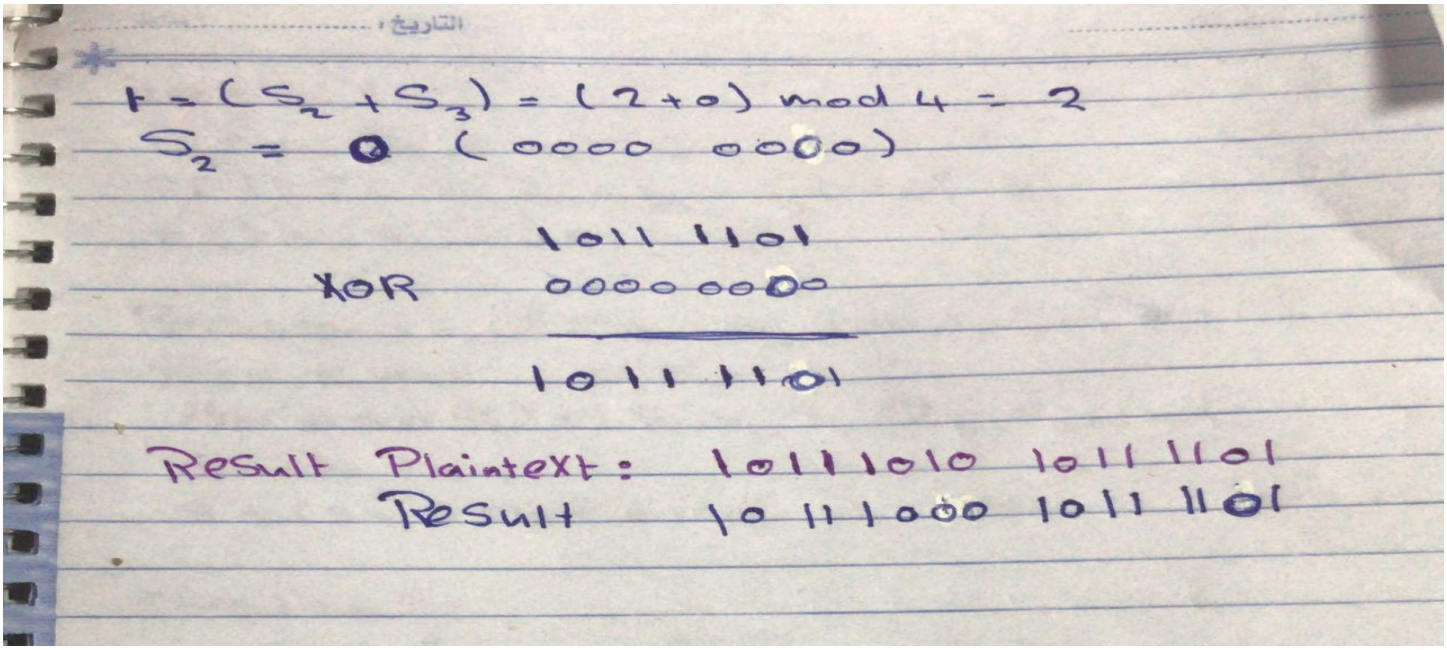
S[] = [S0, S1, S2, S3] = [3, 1, 2, 0]

Because i = (i + 1) mod 4 = 2

f = (f + S2) mod 4 = (1 + 2) mod 4 = 3

Swap S2 with S3

New array S[] = [S0, S1, S2, S3] = [3, 1, 0, 2]



g) Message authentication is one of the services used to counter security attacks. Identify three different methods used. For each method give an example clarifying different approaches used to achieve message authentication and its application conditions.

Answer:

Then three alternative functions used:

- **Message encryption:** Only the sender and receiver should share a key

  -Using Encryption

  - Assume only sender and receiver share a key
  - Then a correctly encrypted message should be from the sender

  Usually also contains error-detection code, sequence number and time stamp

- **Message Authentication Code (MAC)**
  - Small block of data that is appended to the message
  - MAC is generated by using a secret key
  - Assumes both parties A,B share common secret key K_{AB}
  - Code is function of message and key $MAC_M = F(K_{AB}, M)$
  - Message plus code are transmitted

- **Hash function:** Purpose of the HASH function is to produce a "fingerprint"
  Properties of a HASH function H :
  - H can be applied to a block of data at any size
  - H produces a fixed length output

- H(x) is easy to compute for any given x.
- For any given block x, it is computationally infeasible to find x such that H(x) = h (one-way property)
- For any given block x, it is computationally infeasible to find with H(y) = H(x). (weak collision resistance)
- It is computationally infeasible to find any pair (x, y) such that H(x) = H(y) (strong collsion resistance)

h) Discuss the reasons for the introduction of the public-key cryptosystem.

Answer:

Developed to address two key issues:

- Key distribution – how to have secure communications in general without having to trust a KDC with your key
- Digital signatures – how to verify a massage comes intact from the claimed sender

i) In a public-key system using RSA, you intercept the cipher text C = 26 sent to a user whose public key is e = 5, n = 35. What is the plaintext M?

Answer:

First: p = 7 , q =5 **based on** n = p*q = 5*7=35
Second: $\phi(n) = (p-1)(q-1)=(5-1)(7-1)= 4*6 = 24$
Third: $d \equiv e^{-1} \bmod \phi(n) = 5$
Fourth: $M = C^d \bmod n = 26^5 \bmod 35 = 31$

j) Employees are connecting to company networks remotely via mobile devices such as laptops, tablets and smartphones. Remote access needs to satisfy five essential requirements to be efficient and secure. Identify and briefly explain each of these five requirements.

Answer:

- Authentication – validates that the data was sent from the sender.
- Access Control – preventing unauthorized users from accessing the network.

- Confidentiality – preventing the data from being read or copied as the data is being transported.
- Data Integrity – ensuring that the data has not been altered.
- Availability – ensuring that a connection can be made.

k) Justify why SSL can be adapted as a good tool for online web security.

Answer:

1. SSL Protects Data
The core function of an SSL certificate is to protect server-client communication. On installing SSL, every bit of information is encrypted.

2. SSL Affirms Your Identity
The second primary task of an SSL certificate is to provide authentication to a website. Identity verification is one of the most important aspects as far as web security is concerned.

3. Better Search Engine Ranking.

4. SSL Helps You Satisfy PCI/DSS Requirements
If you accept online payments, you must know a thing or two about PCI/DSS requirements.

5. SSL Improves Customer Trust
If it were up to us, we'd have renamed SSL (Secure Socket Layer) to TTL (Trust Transmitting Layer).

l) Consider the following threats to Web security and describe how each is countered by a particular feature of SSL.

Answer:

1. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.

Given that both RC4 and RC2 ciphers have 128-bit encryption, they each have approximately $3.4 * 10^{38}$ possible keys, making them very difficult to crack. Assuming that a hacker could test 10,000 (10^4) keys every second, it could take up to one octillian ($1.08 * 10^{27}$) years to break the cipher. Only when an octillian keys can be tested every second, is it possible that the cipher can be broken within a year.

2. Known Plaintext Dictionary Attack: Many messages will contain predictable plaintext, such as the HTTP GET command. An attacker constructs a dictionary containing every possible encryption of the known-plaintext message. When an encrypted message is intercepted, the attacker takes the portion containing the encrypted known plaintext and looks up the ciphertext in the dictionary. The ciphertext should match against an entry that was encrypted with the same secret key. If there are several matches, each of these can be tried against the full ciphertext to determine the right one. This attack is especially effective against small key sizes (e.g., 40-bit keys).

This attack is defeated the same way the earlier attack is addressed. Since there are so many different sets of keys available, the size of the dictionary required would be too large to be created. For small key sizes, it could be possible to hack into after a certain amount of time, resources and money. However, for larger key sizes, specifically 128-bit, it could take a very long time.

3. Replay Attack: Earlier SSL handshake messages are replayed.

The replay attack is countered through the usage of a timestamp in the server authentication process. The client will check to see if the server's certificate is valid and during that process, a timestamp would be used to verify that the messages are not old.

4. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client.

The client application checks the server domain name specified in the server certificate is the same as the actual domain name of the server. If they are not the same, the authentication fails.

5. Password Sniffing: Passwords in HTTP or other application traffic are eavesdropped.

With SSL, key-management is handled well because short-term session keys are generated using random hash number generators. Each direction of communication generates independent keys for the connection as well as for each instance of the connection.

6. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data.

If the server requests client authentication, the SSL protocol requires that the client create a digital signature by creating a one-way hash from randomly generated data during the handshake and known only to the client and server. The hash data is encrypted with the client's private key that corresponds to the public key in the certificate received by the server.

IP hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts.

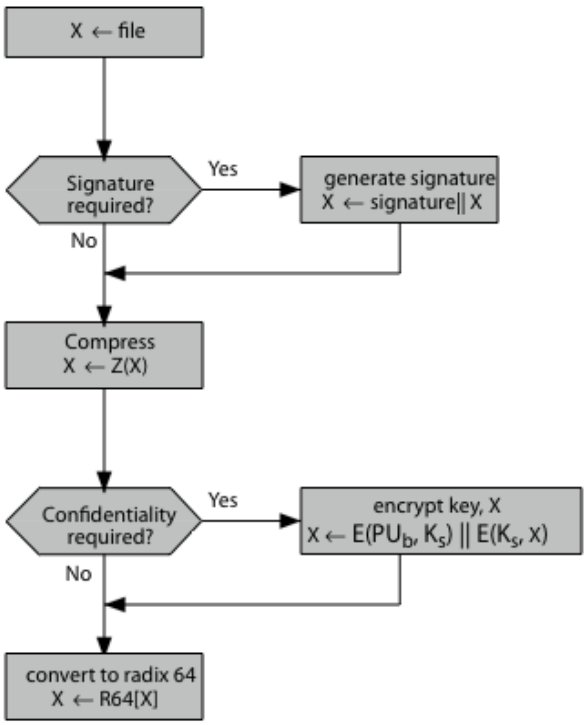
SSL uses HMAC, a simple, fast, hash-based construction with strong theoretical evidence for its security. Authentication can be requested during the connection in order to protect the confidential nature of data being passed.

SYN flooding: An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module typically leaves the 'half-open connection' around for a few minutes. Repeated SYN messages can clog the TCP module.

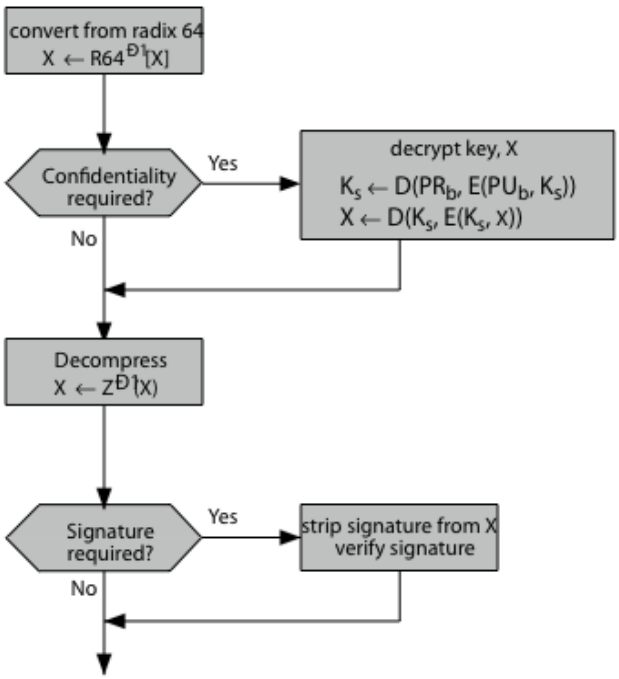
SYN flooding is also handled by SSL in that the source of the message has to be authenticated before a response is generated. The messages that are continuously sent, can be removed if the source of the requests are considered invalid.

m) Discuss using suitable diagram how the five principal services provided by PGP is used for e mail security. If you wished to enhance this service, explain how this could be achieved.

Answer:



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

n) Why does PGP generate a signature before applying compression?

Answer:

- The signature is generated before compression for the reasons shown:
  - so can store uncompressed message & signature for later verification
  - & because compression is non deterministic