

Question Paper

Cryptography and Computer Security (MB361IT) : January 2008

Section A : Basic Concepts (30 Marks)

- This section consists of questions with serial number 1 - 30.
- Answer all questions.
- Each question carries one mark.
- Maximum time for answering Section A is 30 Minutes.

1. Which of the following aspects of information security implies any action that comprises the security of information owned by an organization?

[<Answer>](#)

- (a) Security recovery
- (b) Security attack
- (c) Security service
- (d) Security prevention
- (e) Security identification.


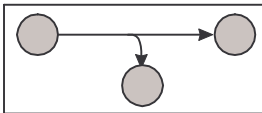
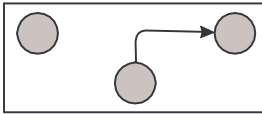
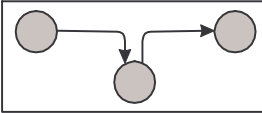

2. In which of the following security threats, an unauthorized party inserts counterfeit objects into the system?

[<Answer>](#)

- (a) Interruption
- (b) Interception
- (c) Concurrence
- (d) Modification
- (e) Fabrication.

3. Which of the following figures of security threat represents interception?

[<Answer>](#)

- (a) 
- (b) 
- (c) 
- (d) 
- (e) 

4. Which of the following active attacks takes place when one entity pretends to be a different entity?

[<Answer>](#)

- (a) Masquerade
- (b) Replay
- (c) Modification of messages
- (d) Denial of service
- (e) Traffic analysis.

5. Which of the following organization is a protocol engineering and development arm of the internet?

[<Answer>](#)

- (a) Internet Architecture Board

- (b) Internet Engineering Board
(c) Internet Engineering Steering Group
(d) Internet Engineering Task Force
(e) Internet Architecture Steering Group.
6. If two parties A and B share a common secret key K_{AB} and when A has a message to be send to B then message authentication code, MAC_M is calculated as [<Answer>](#)
- (a) $F(K_{AB}, M)$
(b) $F(K_{AB}, M_{AB})$
(c) $F(M_A, M_B)$
(d) $F(K_{AB} \times M_{AB})$
(e) $F(K_{AB} / M_{AB})$.
7. A hash function(H) is to produce a “finger print” of a file that satisfies the following five properties is referred as [<Answer>](#)
- H can be applied to a block of data of any size.
 - H produces a fixed-length output.
 - $H(x)$ is relatively easy to compute for any given x, making both hardware and software implementations practical.
 - For any given code h, it is computationally infeasible to find x such that $H(x) = h$.
 - For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.
- (a) Strong hash function
(b) Weak hash function
(c) Virtual hash function
(d) Dependent hash function
(e) Independent hash function.
8. Public-key cryptography algorithm DSS is designed to provide only the digital signature function. DSS stands for [<Answer>](#)
- (a) Data Support Systems
(b) Decision Standard Systems
(c) Digital Signature Standard
(d) Digital Support Systems
(e) Distributed Signature Standard.
9. In PGP, which of the following indicates decompression? [<Answer>](#)
- (a) C
(b) C^{-1}
(c) Z
(d) Z^{-1}
(e) D.
10. The number of additive constants used in MD5 algorithm are [<Answer>](#)
- (a) 4
(b) 8
(c) 16
(d) 32
(e) 64.
11. Which of the following Kerberos version5 flags tells Ticket-Granting-Server (TGS) that a postdated ticket may be issued based on this ticket-granting ticket? [<Answer>](#)
- (a) MAY-POSTDATE
(b) PROXIABLE
(c) PRE-AUTHENT
(d) HW-AUTHENT
(e) POSTDATED.
12. Content-Transfer-Encoding field can actually take on six values. In which of the following Content-Transfer-Encoding value, all the data is represented by short lines of ASCII characters? [<Answer>](#)

- (a) 7 bit
(b) 8 bit
(c) quoted-printable
(d) base64
(e) x-token.
13. Which of the following IPSec documents specify an overview of a security architecture? [<Answer>](#)
- (a) RFC 2401
(b) RFC 2402
(c) RFC 2104
(d) RFC 2406
(e) RFC 2408.
14. In IPSec Encapsulating Security Payload (ESP) format, Security Parameters Index field consists of [<Answer>](#)
- (a) 8 bits
(b) 32 bits
(c) 64 bits
(d) 128 bits
(e) 256 bits.
15. The default automated key management protocol for IPSec is referred to as Internet Security Association and Key Management Protocol (ISAKMP). In ISAKMP header format, what is the size of Initiator Cookie field? [<Answer>](#)
- (a) 8 bits
(b) 32 bits
(c) 64 bits
(d) 128 bits
(e) 256 bits.
16. The default automated key management protocol for IPSec is referred to as Internet Security Association and Key Management Protocol (ISAKMP). Which of the following ISAKMP Payload types indicate protocol for Security Association (SA) for which services and mechanisms are being negotiated? [<Answer>](#)
- (a) Proposal
(b) Transform
(c) Key Exchange
(d) Delete
(e) Nonce.
17. Which of the following classes of intruder is/are likely to be outsider? [<Answer>](#)
- I. Masquerader.
II. Misfeasor.
III. Clandestine user.
- (a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (I) and (II) above
(e) All (I), (II) and (III) above.
18. Which of the following ingredients of conventional encryption scheme performs various substitutions and transformations on the plain text? [<Answer>](#)
- (a) Secret key
(b) Encryption algorithm
(c) Decryption algorithm
(d) Cipher text
(e) Block text.
19. TDEA Conventional encryption algorithm was first proposed by [<Answer>](#)
- (a) Martin
(b) Gailly
(c) Tauchman
(d) Bruce
(e) Richard.
20. What is the key size of the conventional encryption algorithm DES? [<Answer>](#)

- (a) 42 bits
- (b) 56 bits
- (c) 112 bits
- (d) 128 bits
- (e) 168 bits.

21. What is the maximum message size of SHA-1 algorithm?

[<Answer>](#)

- (a) ∞
- (b) $2^{64} - 1$ bits
- (c) $2^{32} + 1$ bits
- (d) $2^{64} + 1$ bits
- (e) $2^{32} - 1$ bits.

22. The maximum ticket lifetime value in Kerberos version 4 is

[<Answer>](#)

- (a) 1280 minutes
- (b) 20 hours
- (c) 70000 seconds
- (d) 1600 minutes
- (e) 15 hours.

23. PGP provides various functions. Which of the following algorithms is used for the function “message encryption” in PGP?

[<Answer>](#)

- (a) DSS
- (b) CAST
- (c) Radix-64 conversion
- (d) ZIP
- (e) SHA.

24. Which of the following key(s) does the Pretty Good Privacy (PGP) use?

[<Answer>](#)

- I. One-time session conventional keys.
- II. Public keys.
- III. Private keys.
- IV. Passphrase-based conventional keys.

- (a) Only (I) above
- (b) Both (I) and (III) above
- (c) Both (II) and (IV) above
- (d) (I), (III) and (IV) above
- (e) All (I), (II), (III) and (IV) above.

25. Which of the following are the components included in signature component of PGP message format?

[<Answer>](#)

- I. Timestamp.
- II. Message digest.
- III. Leading two octets of message digest.
- IV. Key ID of sender's public key.

- (a) Both (I) and (III) above
- (b) Both (II) and (IV) above
- (c) (I), (II) and (IV) above
- (d) (I), (III) and (IV) above
- (e) All (I), (II), (III) and (IV) above.

26. Which type of virus is explicitly designed to hide itself from detection by antivirus software?

[<Answer>](#)

- (a) Parasitic virus
- (b) Memory-resident virus
- (c) Polymorphic virus
- (d) Stealth virus
- (e) Boot sector virus.

27. In which of the following phase, the virus is activated to perform the function for which it was intended?

[<Answer>](#)

- (a) Delay phase
- (b) Dormant phase
- (c) Propagation phase

- (c) Propagation phase
- (d) Triggering phase
- (e) Execution phase.

28. Which of the following defines a framework for the provision of authentication services by the X.500 directory to its users?

[<Answer>](#)

- (a) Z.509
- (b) Kerberos
- (c) X.509
- (d) S/MIME
- (e) MIME.

29. Which of the following is **not** a technique of password selection?

[<Answer>](#)

- (a) User education
- (b) Administrator password checking
- (c) Reactive password checking
- (d) Proactive password checking
- (e) Computer-generated passwords.

30. In which of the following, both sender and receiver use the same key?

[<Answer>](#)

- (a) Symmetric conventional encryption
- (b) Asymmetric encryption
- (c) RSA public key encryption
- (d) DSS public key encryption
- (e) Elliptic curve encryption.

END OF SECTION A

Section B : Problems/Caselet (50 Marks)

- This section consists of questions with serial number 1 – 5 .
- Answer all questions.
- Marks are indicated against each question.
- Detailed workings/explanations should form part of your answer.
- Do not spend more than 110 - 120 minutes on Section B.

1. a. Explain about RSA algorithm. (6 marks) [<Answer>](#)
 b. Given $p=7$, $q=11$, $e=17$, $M=8$. Find the following, using RSA algorithm.
 i. Key generation.
 ii. Encryption.
 iii. Decryption. (8 marks) [<Answer>](#)
2. Given $n=11$ and the encoding,

A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11

 Plaintext: B I ? = 1 7 ?
 Cipher text: J F A = 8 5 0

 Where, $m * K_1 + K_0 \bmod 11 = c$.
 a. Solve for K_0 and K_1 . (5 marks)
 b. Determine the remaining plaintext character. (5 marks) [<Answer>](#)
3. a. Explain about Diffie-Hellman key exchange algorithm. (6 marks) [<Answer>](#)
 b. Consider a Diffie-Hellman scheme with a common prime $q=11$ and a primitive root $\alpha=2$.
 i. If user A has public key $Y_A=9$, what is A's private key X_A ?
 ii. If user B has public key $Y_B=3$, what is the shared secret key K? (8 marks)

Caselet

Read the caselet carefully and answer the following questions:

4. What types of threats the systems of NFS likely to face? (8 marks) [<Answer>](#)
5. What are the methods available to counteract such types of threats in network security? Explain. (4 marks) [<Answer>](#)

National Financial Services (NFS) is a premier financial services provider. NFS employs around 2700 people for its operations. Most of them are busy working for client's transactions, making payments, dealing with brokerage firms, granting loans and credits, the foreign exchange dealings etc. All these transactions are done online.

Recently the company has seen a report published by the Gartner IT research group, which stated that US financial institutions lost around USD2.4 billion in one year due to fraud, much of which is associated with on-line transactions. The Gartner study was based on a survey of 5,000 Internet users in the US.

In most cases it was not an insider's job. Thieves stole account numbers and passwords to get into accounts on-line or through telephone banking services. It did not involve face-to-face transactions. Much of the crime was the result of so-called phishing attacks, or e-mail scams that lure users to fake Web sites or that upload key logging applications on users' PCs.

Frightened with the reports the bank has assessed its online security and to its surprise it has found

that the company did not employ any security systems as such.

END OF CASELET

END OF SECTION B

Section C : Applied Theory (20 Marks)

- This section consists of questions with serial number 6 - 7 .
- Answer all questions.
- Marks are indicated against each question.
- Do not spend more than 25 - 30 minutes on Section C.

6. What are the approaches to message authentication? Explain. (10 marks)

[<Answer>](#)

7. Pretty Good Privacy (PGP) provides confidentiality and authentication service that can be used for electronic mail and file storage applications. Discuss various PGP services. (10 marks)

[<Answer>](#)

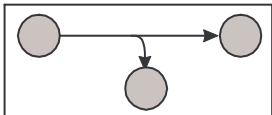
END OF SECTION C

END OF QUESTION PAPER

Suggested Answers

Cryptography and Computer Security (MB361IT) : January 2008

Section A : Basic Concepts

- | Answer | Reason | |
|--------|---|-----------------------------|
| 1. B | Security attack: Any action that comprises the security of information owned by an organization. So, option (b) is the answer. | <TOP> |
| 2. E | Fabrication: An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity.
Interruption: An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability.
Interception: An authorized party gains access to an asset. This is an attack on confidentiality.
Modification: An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity.
Concurrence is not the category of attack.
So, option (e) is the answer. | <TOP> |
| 3. B |  represents interception.
So, option (b) is the answer. | <TOP> |
| 4. A | Masquerade takes place when one entity pretends to be a different entity. | <TOP> |

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Modification of message contents means that some portion of a legitimate message is altered or that messages are delayed or recorded to produce an unauthorized effect.

Denial of service prevents or inhibits the normal use or management of communications facilities.

Traffic analysis is a passive attack.

So option (a) is the answer.

5. D Internet Engineering Task Force is a protocol engineering and development arm of the internet. [< TOP >](#)
So, option (d) is the answer.
6. A If two parties A and B share a common secret key K_{AB} and when A has a message to send to B, then message authentication code, MAC_M is calculated as $F(K_{AB}, M)$. [< TOP >](#)
So, option (a) is the answer.
7. B A hash function (H) is to produce a “finger print” of a file that satisfies the following five properties is called Weak hash function. [< TOP >](#)
1. H can be applied to a block of data of any size.
2. H produces a fixed-length output.
3. $H(x)$ is relatively easy to compute for any given x, making both hardware and software implementations practical.
4. For any given code h, it is computationally infeasible to find x such that $H(x)=h$.
5. For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y)=H(x)$.
So, option (b) is the answer.
8. C DSS stands for Digital Signature Standard. [< TOP >](#)
So, option (c) is the answer.
9. D In PGP, decompression is represented as Z^{-1} . [< TOP >](#)
So, option (d) is the answer.
10. E The number of additive constants used in MD5 algorithm are 64. [< TOP >](#)
So, option (e) is the answer.
11. A MAY-POSTDATE flag tells Ticket-Granting-Server that a postdated ticket may be issued based on this ticket-granting ticket. [< TOP >](#)
PROXIABLE flag tells Ticket-Granting-Server that a new ticket with a different network address may be issued based on the presented ticket.
POSTDATED flag indicates that ticket has been postdated; the end server can check the authtime field to see when the original authentication occurred.
HW-AUTHENT is the protocol employed for initial authentication required the use of hardware expected to be possessed solely by the named client.
PRE-AUTHENT comes during initial authentication, the client was authenticated by the KDC (Key Distribution Center) before a ticket was issued.
So, option (a) is the answer.
12. A In 7bit, the data are all represented by short lines of ASCII characters. [< TOP >](#)
base64: encodes data by mapping 6-bit blocks of input to 8-bit blocks of output.
The x-token is a named nonstandard encoding.
In 8bit, the lines are short, but there may be non-ASCII characters.
quoted-printable: encodes the data in such a way that if the data being encoded are mostly ASCII text, the encoded form of the data remains largely recognizable by humans.
So, option (a) is the answer.
13. A RFC 2401 specifies an overview of a security architecture. [< TOP >](#)
So, option (a) is the answer.
14. B In IPSec Encapsulating Security Payload (ESP) format, Security Parameters Index field consists of 32 bits. [< TOP >](#)

So, option (b) is the answer.

15. C In ISAKMP, the size of Initiator Cookie field is 64 bits. [< TOP >](#)
So, option (c) is the answer.
16. A Proposal Payload type indicate protocol for Security Association (SA) for which services and mechanisms are being negotiated. [< TOP >](#)
Delete Payload type indicates Security Association (SA) that is no longer valid.
Transform Payload type indicates transform and related SA attributes.
Key Exchange Payload type supports a variety of key exchange techniques.
Nonce Payload type contains a nonce.
So, option (a) is the answer.
17. A Masquerader is likely to be an outsider. [< TOP >](#)
Misfeasor generally is an insider.
Clandestine user can be either an outsider or an insider.
So, option (a) is the answer.
18. B Encryption algorithm performs various substitutions and transformations on the plain text. [< TOP >](#)
So, option (b) is the answer.
19. C TDEA Conventional encryption algorithm was first proposed by Tauchman. [< TOP >](#)
So, option (c) is the answer.
20. B Key size of the conventional encryption algorithm DES is 56 bits. [< TOP >](#)
So, option (b) is the answer.
21. B Maximum message size of SHA-1 algorithm is $2^{64} - 1$ bits. [< TOP >](#)
So, option (b) is the answer.
22. A The maximum ticket lifetime value in Kerberos version 4 is $2^8 \times 5 = 1280$ minutes or a little over 21 hours or 76800 seconds. [< TOP >](#)
So, option (a) is the answer.
23. B The function of CAST algorithm is Message encryption. [< TOP >](#)
So, option (b) is the answer.
24. E PGP makes use of the following keys: [< TOP >](#)
I. One-time session conventional keys.
II. Public keys.
III. Private keys.
IV. Passphrase-based conventional keys.
So, option (e) is the answer.
25. E Components included in signature component of PGP message format are: [< TOP >](#)
I. Timestamp.
II. Message digest.
III. Leading two octets of message digest.
IV. Key ID of sender's public key.
So, option (e) is the answer.
26. D Stealth virus is a form of virus explicitly designed to hide itself from detection by antivirus software. [< TOP >](#)
So, option (d) is the answer.
27. D In Triggering phase, virus is activated to perform the function for which it was intended. [< TOP >](#)
So, option (d) is the answer.
28. C X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. [< TOP >](#)
So, option (c) is the answer.
29. B Administrator password checking is not a technique of password selection. [< TOP >](#)

So, option (b) is the answer.

- 30.** A In symmetric conventional encryption both sender and receiver use the same key.
So, option (a) is the answer.

[<TOP>](#)

Section B : Problems/Caselets

1. a. The RSA Public-Key Encryption Algorithm

[< TOP >](#)

One of the first public-key schemes was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978. The RSA scheme has since that time reigned supreme as the most widely accepted and implemented approach to public-key encryption. RSA is a block cipher in which the plaintext and ciphertext are integers between 0 and $n-1$ for some n .

Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C :

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Both sender and receiver must know the values of n and e , and only the receiver knows the value of d . This is a public-key encryption algorithm with a public key of $KU = \{e, n\}$ and a private key of $KR = \{d, n\}$. For this algorithm to be satisfactory for public-key encryption, the following requirements must be met:

- It is possible to find values of e, d, n such that $M^{ed} = M \bmod n$ for all $M < n$.
- It is relatively easy to calculate M^e and C for all values of $M < n$.
- It is infeasible to determine d given e and n .

The first two requirements are easily met. The third requirement can be met for large values of e and n .

Begin by selecting two prime numbers, p and q , and calculating their product n , which is the modulus for encryption and decryption. Next, we need the quantity $\phi(n)$, referred to as the Euler quotient of n , which is the number of positive integers less than n and relatively prime to n . Then select an integer e that is relatively prime to $\phi(n)$ [i.e., the greatest common divisor of e and $\phi(n)$ is 1]. Finally, calculate d as the multiplicative inverse of e , modulo $\phi(n)$. It can be shown that d and e have the desired properties.

Suppose that user A has published its public key and that user B wishes to send the message M to A. Then B calculates $C = M^e \bmod n$ and transmits C . On receipt of this ciphertext, user A decrypts by calculating $M = C^d \bmod n$.

The algorithm can be summarized as below:

Key generation

Select p, q p and q both prime

Calculate $n = p \times q$

Calculate $\phi(n) = (p-1)(q-1)$

Select integer e $\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$

Calculate d $d = e^{-1} \bmod \phi(n)$

Public key $KU = \{e, n\}$

Private key $KR = \{d, n\}$

Encryption

Plaintext: $M < n$

Ciphertext: $C = M^e \bmod n$

Decryption

Ciphertext: C

Plaintext: $M = C^d \bmod n$

b. Given $P = 7, q = 11, e = 17, M = 8$

- i. 1. $n = pq$
 $= (7)(11) = 77$
2. $\phi(n) = (p-1)(q-1)$ (Euler's function)
 $= (7-1)(11-1)$

$$= (6)(10) = 60$$

$$3. \quad de = 1 \bmod \phi(n)$$

$$(d)(17) = 1 \bmod 60$$

$$d = 17^{-1} \bmod 60$$

$$\Rightarrow 17(x) = 1 \bmod 60$$

$$\Rightarrow 53$$

[17*x=1mod60, ie, multiplying 17 with x should get a remainder of 1 when divided by 60]

$$\text{Public key} = \{e, n\} = \{17, 77\}$$

$$\text{Private key} = \{d, n\} = \{53, 77\}$$

ii. Encryption

$$c = M^e \bmod n$$

$$= 8^{17} \bmod 77 = 57$$

iii. Decryption

$$M = c^d \bmod n$$

$$= 57^{53} \bmod 77 = 8.$$

2.

[< TOP >](#)

a. Given $m * K_1 + K_0 \bmod 11 = c$,
So,

$$1 * K_1 + K_0 \bmod 11 = 8$$

$$7 * K_1 + K_0 \bmod 11 = 5$$

By solving these two equations, we get

$$6 K_1 = -3$$

$$= -1/2 \bmod 11$$

$$= -1(2^{-1} \bmod 11)$$

$$= -6 \bmod 11$$

$$= (11-6)$$

$$= 5$$

[2*x=1mod11, ie, multiplying 2 with x should get a remainder of 1 when divided by 11]

$$\therefore K_1 + K_0 \bmod 11 = 8$$

$$K_0 \bmod 11 = 8 - 5$$

$$K_0 = 3$$

b. $m * K_1 + K_0 \bmod 11 = c$ [let ?=x]

$$5(x) + 3 \bmod 11 = 0$$

$$x = -3/5 \bmod 11$$

$$= -3(5^{-1} \bmod 11)$$

$$= -27 \bmod 11$$

$$= -5 \bmod 11$$

$$= 11 - 5$$

$$= 6$$

[5*x=1mod11, ie, multiplying 5 with x should get a remainder of 1 when divided by 11]

$$\therefore \text{Plaintext: } \quad B \quad I \quad G = 1 \quad 7 \quad 6$$

3. a. **Diffie-Hellman Key Exchange:**

[< TOP >](#)

The first published public-key algorithm appeared in the seminal paper by Diffie and Hellman that defined public-key cryptography is generally referred to as Diffie-Hellman key exchange. A number of commercial

products employ this key exchange technique.

The purpose of the algorithm is to enable two users to exchange a secret key securely that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of the keys.

The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms. Briefly, we can define the discrete logarithm in the following way. First, we define a primitive root of a prime number p as one whose powers generate all the integers from 1 to $p - 1$. That is, if a is a primitive root of the prime number p , then the numbers

$$a \bmod p, a^2 \bmod p, \dots, a^{p-1} \bmod p$$

are distinct and consist of the integers from 1 through $p - 1$ in some permutation.

For any integer b and a primitive root a of prime number p , one can find a unique exponent i such that

$$b = a^i \bmod p, \text{ where } 0 \leq i \leq (p - 1)$$

The exponent i is referred to as the discrete logarithm, or index, of b for the base a , mod p . This value is denoted as $\text{ind}_{a,p}(b)$

There are two publicly known numbers: a prime number q and an integer α that is a primitive root of q . Suppose the users A and B wish to exchange a key. User A selects a random integer $X_A < q$ and computes $Y_A = \alpha^{X_A} \bmod q$. Similarly, user B independently selects a random integer $X_B < q$ and computes $Y_B = \alpha^{X_B} \bmod q$. Each side keeps the X value private and makes the Y value available publicly to the other side. User A computes the key as $K = (Y_B)^{X_A} \bmod q$ and user B computes the key as $K = (Y_A)^{X_B} \bmod q$. These two calculations produce identical results.

Suppose that user A wishes to set up a connection with user B and a secret key to encrypt messages on that connection. User A can generate a one-time private key X_A , calculate Y_A and send that to user B. User B responds by generating a private value X_B , calculating Y_B , and sending Y_B to user A. Both users can now calculate the key. The necessary public values q and α would need to be known ahead of time. Alternatively, user A could pick values for q and α and include in the first message.

The algorithm can be summarized as below:

Global Public Elements

q prime number
 α $\alpha < q$ and α a primitive root of q

User A key generation

Select private X_A $X_A < q$
 Calculate public Y_A $Y_A = \alpha^{X_A} \bmod q$

User B key generation

Select private X_B $X_B < q$
 Calculate Y_B $Y_B = \alpha^{X_B} \bmod q$

Generation of secret key by User A

$$K = (Y_B)^{X_A} \bmod q$$

Generation of secret key by User B

$$K = (Y_A)^{X_B} \bmod q$$

b. From given data $q = 11$, $\alpha = 2$

i. Given $Y_A = 9$

To find X_A , we have

$$Y_A = \alpha^{X_A} \bmod q$$

$$9 = 2^{X_A} \bmod 11 \quad (X_A < 11)$$

$$\therefore X_A = 6$$

ii. Given $Y_B = 3$

To find the shared key, we should know X_B

$$Y_B = \alpha^{X_B} \bmod q$$

$$3 = 2^{X_B} \bmod 11 \quad (X_B < 11)$$

$$X_B = 8.$$

$$\therefore \text{Shared secret key } K = (Y_B)^{X_A} \bmod q \quad (\text{or}) \quad K = (Y_A)^{X_B} \bmod q$$

$$\begin{aligned} K &= 3^6 \bmod 11 \\ &= 729 \bmod 11 = 3 \end{aligned}$$

(or)

$$\begin{aligned} K &= 9^8 \bmod 11 \\ &= 43046721 \bmod 11 = 3 \end{aligned}$$

4. The types of threats that are prone to attack the systems of NFS are:

[< TOP >](#)

The threats come in the form of viruses or take different other forms such as malicious programs, trap doors, logic bomb, Trojan horses.

- **Malicious programs:** These can be classified into two categories – those that need a host program, and those that are independent. The former are essentially fragments of programs that cannot exist independently of some actual application program, utility or system program. The latter are self-contained programs that can be scheduled and run by the operating system.
- **Trap doors:** A trap door is a secret entry point into a program that allows someone that is aware of the trap door to gain access without going through the usual security access procedures. They become threats when they are used by unscrupulous programmers to gain unauthorized access.
- **Logic bombs:** The logic bomb is a code embedded in some legitimate program that is set to ‘explode’ when certain conditions are met. Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files, a particular day of the week or date, or a particular user running the application.
- **Trojan horses:** A Trojan horse is a useful, program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function. Trojan horse programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.
- **Worms:** Network worm programs use network connections to spread from system to system. Once active within a system, a network worm can behave as a computer virus or bacteria, or it could implant Trojan horse programs or perform any number of disruptive or destructive actions.
- **Bacteria:** Bacteria are programs that do not explicitly damage any files. Their sole purpose is to replicate themselves. Bacteria reproduce exponentially, eventually taking up all the processor capacity, memory or disk space, denying users access to those resources.
- **Viruses:** A virus is a program that can ‘infect’ other programs by modifying them; the modification includes a copy of the virus program, which can then go to infect other programs. A virus can do everything that other programs do. The only difference is that it attaches itself to another program and executes secretly when the host program is run. Once a virus is executing, it can perform any function, such as erasing files and programs.

5. Two most commonly used methods in network security are encryption and firewalls.

[< TOP >](#)

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. “software for encryption” can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now used in protecting information within many kinds of civilian systems, such as computers, networks (e.g. the Internet e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. Encryption is also used in digital rights management to restrict the use of copyrighted material and in software copy protection to protect against reverse engineering and software piracy.

Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to verify the integrity and authenticity of a message; for example, a message authentication code (MAC) or digital signatures. Standards and cryptographic software and hardware to perform encryption are widely available, but successfully using encryption to ensure security is a challenging problem.

Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text* ; encrypted data is referred to as *cipher text*.

Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the internet. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system. A firewall is a convenient platform for several Internet functions that are security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function audits or logs Internet usage. A firewall can serve as the platform for IPSec. Using the tunnel mode capability, the firewall can be used to implement virtual private networks.

Section C: Applied Theory

6. Approaches to message authentication:

[< TOP >](#)

Encryption protects against passive attack (eavesdropping). A different requirement is to protect against active attack (falsification of data and transactions). Protection against such attacks is known as message authentication.

A message, file, document, or other collection of data is said to be authentic when it is genuine and came from its alleged source. Message authentication is a procedure that allows communicating parties to verify that received messages are authentic. The two important aspects are to verify that the contents of the message have not been altered and that the source is authentic. We may also wish to verify a message's timeliness (it has not been artificially delayed and replayed) and sequence relative to other messages flowing between two parties.

Authentication Using Conventional Encryption

It is possible to perform authentication simply by the use of conventional encryption. If we assume that only the sender and receiver share a key (which is as it should be), then only the genuine sender would be able to encrypt a message successfully for the other participant. Furthermore, if the message includes an error-detection code and a sequence number, the receiver is assured that no alterations have been made and that sequencing is proper. If the message also includes a timestamp, the receiver is assured that the message has not been delayed beyond that normally expected for network transit.

Message Authentication without Message Encryption

There are several approaches to message authentication that do not rely on encryption. In all of these approaches, an authentication tag is generated and appended to each message for transmission. The message itself is not encrypted and can be read at the destination independent of the authentication function at the destination.

Because the approaches do not encrypt the message, message confidentiality is not provided. Because conventional encryption will provide authentication, and because it is widely used with readily available products, why not simply use such an approach, which provides both confidentiality and authentication? Three situations are suggested in which message authentication without confidentiality is preferable:

1. There are a number of applications in which the same message is broadcast to a number of destinations (for example, notification to users that the network is now unavailable or an alarm signal in a control center). It is cheaper and more reliable to have only one destination responsible for monitoring authenticity. Thus, the message must be broadcast in plaintext with an associated message authentication tag. The responsible system performs authentication. If a violation occurs, the other destination systems are alerted by a general alarm.
2. Another possible scenario is an exchange in which one side has a heavy load and cannot afford the time to decrypt all incoming messages. Authentication is carried out on a selective basis, and messages are chosen at random for checking.
3. Authentication of a computer program in plaintext is an attractive service. The computer program can be executed without having to decrypt it every time, which would be wasteful of processor resources. However, if a message authentication tag were attached to the program, it could be checked whenever assurance is required of the integrity of the program.

Thus, there is a place for both authentication and encryption in meeting security requirements.

Message Authentication Code (MAC)

One authentication technique involves the use of a secret key to generate a small, block of data, known as a message authentication code, that is appended to the message. This technique assumes that two communicating parties, say A and B, share a common secret key K_{AB} . When A has a message to send to B, it calculates the message authentication code as a function of the message and the key: $MAC_M = F(K_{AB}, M)$. The message plus code are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new message authentication code. The received code is compared to the calculated code (Figure). If we assume that only the receiver and the sender know the identity of the secret key, and if the received code matches the calculated code, then

1. The receiver is assured that the message has not been altered. If an attacker alters the message but does not alter the code, then the receiver's calculation of the code will differ from the received code. Because the attacker is assumed not to know the secret key, the attacker cannot alter the code to correspond to the alterations in the message.
2. The receiver is assured that the message is from the alleged sender. Because no one else knows the secret key, no one else could prepare a message with a proper code.
3. If the message includes a sequence number (such as is used with X.25, HDLC and TCP), then the receiver can be assured of the proper sequence, because an attacker cannot successfully alter the sequence number.

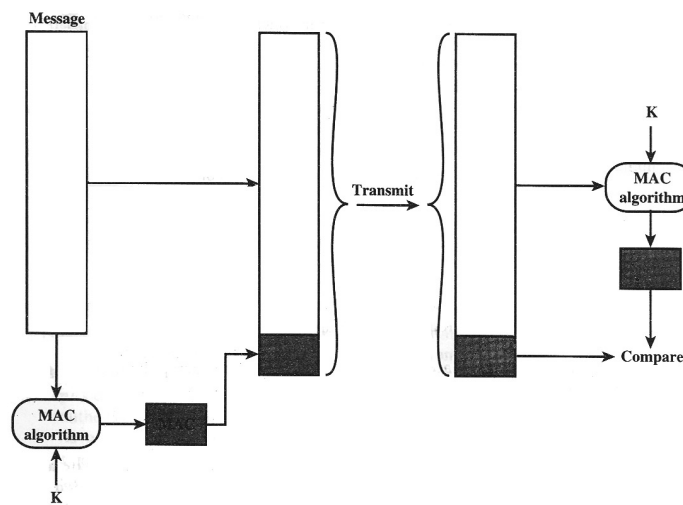


Fig: Message authentication using a message authentication code (MAC)

A number of algorithms could be used to generate the code. The National Bureau of Standards, in its publication *DES Modes of Operation*, recommends the use of DEA. DEA is used to generate an encrypted version of the message and the last number of bits of ciphertext are used as the code. A 16- or 32-bit code is typical.

The process just described is similar to encryption. One difference is that the authentication algorithm need not be reversible, as it must for decryption. It turns out that because of the mathematical properties of the authentication function, it is less vulnerable to being broken than encryption.

One-Way Hash Function

A variation on the message authentication code that has received much attention recently is the one-way hash function. As with the message authentication code, a hash function accepts a variable-size message M as input and produces a fixed-size message digest $H(M)$ as output. Unlike the MAC, a hash function does not also take a secret key as input. To authenticate a message, the message digest is sent with the message in such a way that the message digest is authentic.

The below figure illustrates 3 ways in which the message can be authenticated. The message digest can be encrypted using conventional encryption; if it is assumed that only the sender and receiver share the encryption key, then authenticity is assured. The message can also be encrypted using public-key encryption. The public-key approach has two advantages: It provides a digital signature as well as message authentication; and it does not require the distribution of keys to communicating parties.

These two approaches have an advantage over approaches that encrypt the entire message in that less computation is required. Nevertheless, there has been interest in developing a technique that avoids encryption altogether. Several reasons for this interest are pointed out:

- Encryption software is quite slow. Even though the amount of data to be encrypted per message is small, there may be a steady stream of messages into and out of a system.
- Encryption hardware costs are nonnegligible. Low-cost chip implementations of DES are

available, but the cost adds up if all nodes in a network must have this capability.

- Encryption hardware is optimized toward large data sizes. For small blocks of data, a high proportion of the time is spent in initialization/invocation overhead.
- Encryption algorithms may be covered by patents. Some encryption algorithms, such as the RSA public-key algorithm, are patented and must be licensed, adding a cost.
- Encryption algorithms may be subject to export control. This is true of DES.

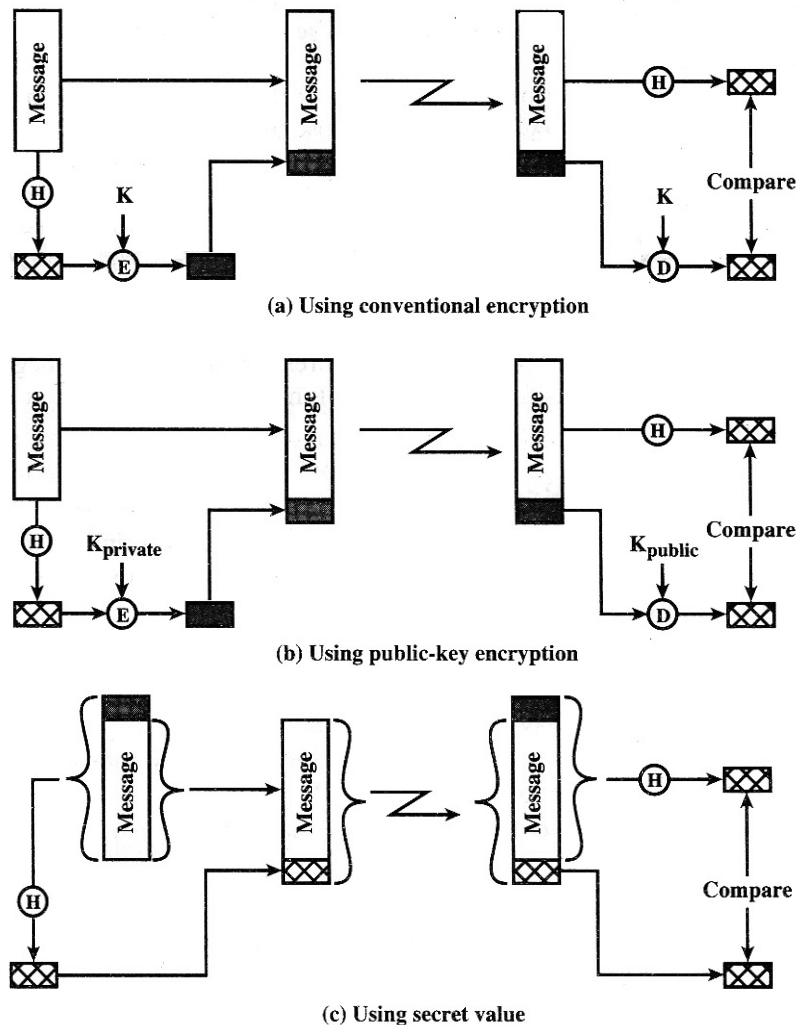


Fig: Message Authentication Using a One-Way Hash Function

Figure shows a technique that uses a hash function but no encryption for message authentication. This technique assumes that two communicating parties, say A and B, share a common secret value S_{AB} . When A has a message to send to B, it calculates the hash function over the concatenation of the secret value and the message: $MD_M = H(S_{AB} || M)$. It then sends $[M || MD_M]$ to B. Because B possesses S_{AB} , it can recompute $H(S_{AB} || M)$ and verify MD_M . Because the secret value itself is not sent, it is not possible for an attacker to modify an intercepted message. As long as the secret value remains secret, it is also not possible for an attacker to generate a false message.

A variation on the third technique, called HMAC, is the one adopted for IP security; it has also been specified for SNMPv3.

7. Pretty Good Privacy (PGP) consists of five services: authentication, confidentiality, compression, e-mail compatibility and segmentation.

[< TOP >](#)

Summary of PGP Services.

Function	Algorithms Used	Description

Message encryption	CAST or IDEA or three-key triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed, for storage or transmission, using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.
Segmentation	–	To accommodate maximum message size limitations, PGP performs segmentation and reassembly.

[< TOP OF THE DOCUMENT >](#)