Important Questions

Two Marks

1] State whether symmetric and asymmetric cryptographic algorithms need key exchange?

Both symmetric and asymmetric cryptographic algorithms require key exchange. Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key.

2] In the elliptic curve group defined by $y_2= x_3- 17x + 16$ over real numbers, what is $P + Q$ if $P = (0,-4)$ and $Q = (1, 0)$?

Solution:

$$y_2= x_3- 17x + 16$$

From the Addition Formulae:

$$\lambda = y_2 - y_1/ x_2 - x_1$$
$$= 0-(-4)/(1-0)$$
$$\lambda = 4$$
$$x_3 = \lambda^2 - x_1-x_2$$
$$= 4^2-0-1$$
$$=16-1$$
$$=15$$
$$y_3= \lambda(x_1-x_3)-y_1$$
$$=4(0-15)-(-4)$$
$$=-60+4$$
$$= - 56$$

Answer: $P + Q = (15 , -56)$

3] Specify the requirements for message authentication.

- Disclosure
- Traffic analysis
- Masquerade
- Content identification
- Sequence modification
- Timing modification
- Source repudiation
- Destination repudiation

4] Define hashing function.

Hash function accepts a variable size message M as input and produces a fixed-size output, referred to as hash code H(M). A hash code does not use a key but is a function only of the input message. The hash code is also referred to as a message digest or hash value.

A hash value h is generated by a function H of the form

$$\mathbf{h = H(M)}$$

where M is a variable-length message and H(M) is the fixed-length hash value.

5] What are the properties of hashing function in cryptography?

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 value h, it is computationally infeasible to find x such that H(x) = h. This is sometimes referred to as the **one-way property**.

5. For any given block x, it is computationally infeasible to find y x such that H(y) = H(x). This is sometimes referred to as **weak collision resistance**.
6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y). This is sometimes referred to as **strong collision resistance**.

6] How a digital signature differs from authentication protocols?

Authentication is about verifying that the user is who he claims to be. A digital signature is about protecting the integrity of certain data and asserting that the data originated from a certain user.

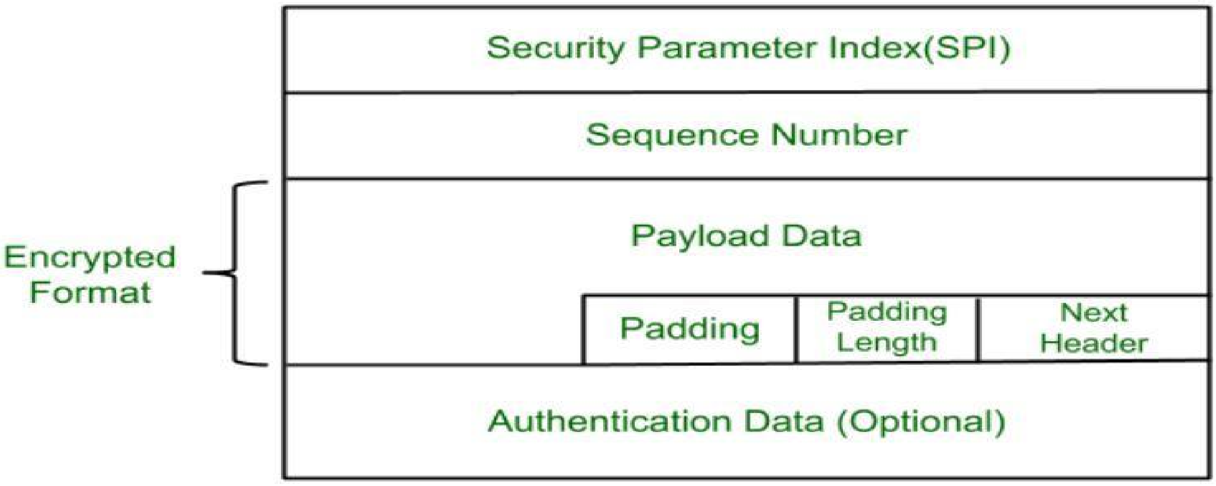
7] Outline the requirements of Kerberos.

- **Secure:** A network eavesdropper should not be able to obtain the necessary information to impersonate a user.
- **Reliable**: For all services that rely on Kerberos for access control, lack of availability of the Kerberos service means lack of availability of the supported services.
- **Transparent:** Ideally, the user should not be aware that authentication is taking place, beyond the requirement to enter a password.
- **Scalable:** The system should be capable of supporting large numbers of clients and servers. This suggests a modular, distributed architecture.

8] Interpret whether E-mail compatibility function in PGP is needed.

When PGP is used, at least part of the block to be transmitted is encrypted. If only the signature service is used, then the message digest is encrypted. If the confidentiality service is used, the message plus signature are encrypted.

9] Draw the General format of IPsec ESP.



10] Define Intruder and List Classes of Intruders.

An individual who gains, or attempts to gain, unauthorized access to a computer system or to gain unauthorized privileges on that system.

- ✔ Masquerader
- ✔ Misfeasor
- ✔ Clandestine user

11] Mention the Factoring Problem involved in the RSA algorithm.

Three approaches can be identified to attacking RSA mathematically.

1. Factor n into its two prime factors. This enables calculation of $\phi(n)$ $\phi(n)$ = (p - 1) × (q - 1), which in turn enables determination of $d \equiv e^{-1}(mod\ \phi(n))$ $d \equiv e^{-1}(mod\ \phi(n))$.
2. Determine $\phi(n)$ $\phi(n)$ directly, without first determining p and q. Again, this enables determination of $d \equiv e^{-1}(mod\ \phi(n))$ $d \equiv e^{-1}(mod\ \phi(n))$.
3. Determine d directly, without first determining $\phi(n)$ $\phi(n)$.

12] Define Elliptic curves over Zp.

Elliptic curve cryptography makes use of elliptic curves in which the variables an coefficients are all restricted to elements of a finite field. Two families of elliptic curves are used in cryptographic applications: prime curves over Zp and binary curves over GF(2m). For a prime curve over Zp, we use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through p - 1 and in which calculations are performed modulo p.

13] Define message digest.

When a hash function is used to provide message authentication, the hash function value is often referred to as a **message digest**. The hash code is a function of all the bits of the message and provides an error-detection capability: A change to any bit or bits in the message results in a change to the hash code.

14] Define: SET

Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transactions on the Internet.

- ✔ Confidentiality of information
- ✔ Integrity of data
- ✔ Cardholder account authentication
- ✔ Merchant authentication

Big Questions:

1. Perform Encryption and Decryption for the RSA algorithm parameters p=3, q=11, e=7, d=?, M=5
2. Demonstrate encryption and decryption to the system with p=7, q=11, e=17, M=8
3. MD5 algorithm
4. DSA(DSS)
5. PGP
6. Secure Electronic Transaction (SET)
7. Firewall characteristics and types of firewalls.
8. Message Authentication Code (MAC) with security
9. Hash functions with security
10. Kerberos authentication service

Apply the MAC on the Cryptographic checksum method to authenticate build confidentiality of the message where the authentication is tied to the message M = 8376, K1 = 4892 and K2 = 53624071.

Steps (7)

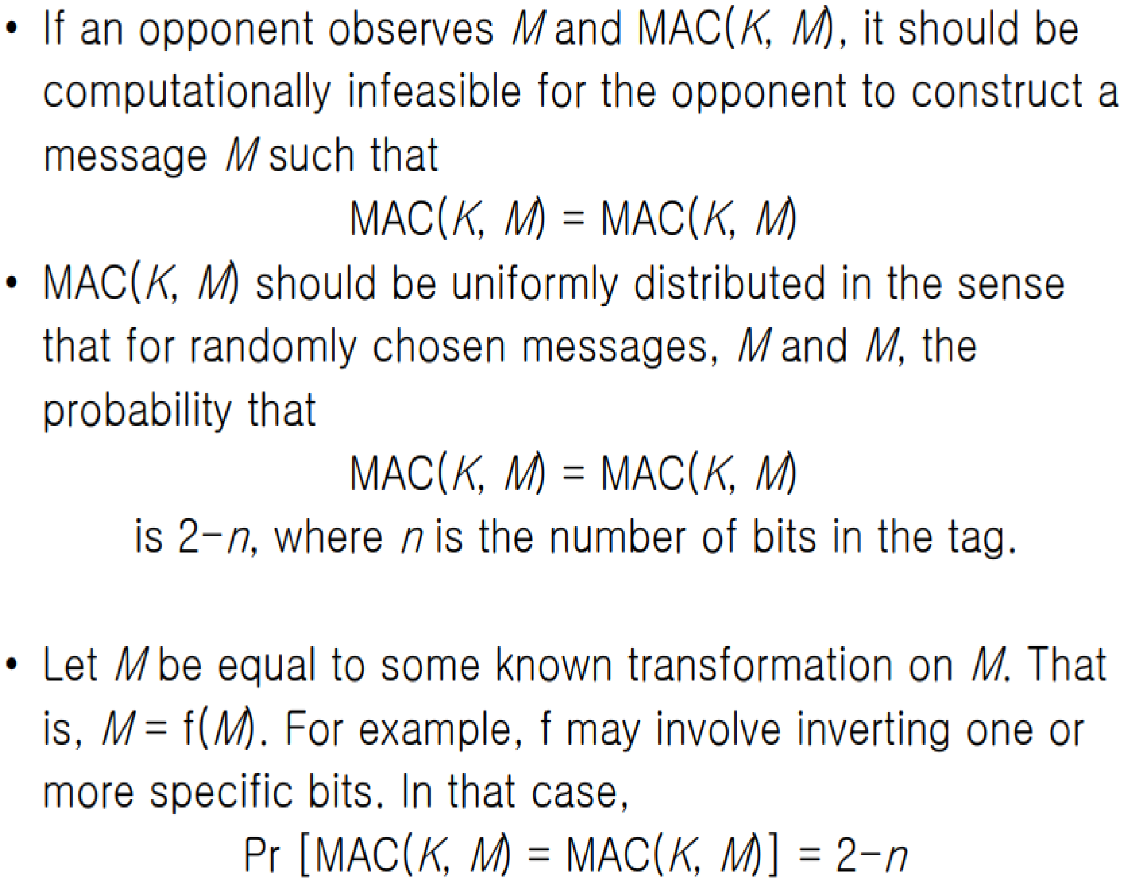
Problem solution (8)

This technique assumes that two communicating parties, say A and B, share a common secret key K. When A has a message to send to B, it calculates the MAC as a function of the message and the key MAC = C(K, M)

M = input message
C = MAC function
K = shared secret key
MAC = message authentication code

There are a number of applications in which the same message is broadcast to a number of destinations

- An exchange in which one side has a heavy load and cannot afford the time to decrypt all incoming messages
- The computer program can be executed without having to decrypt it every time, which would be wasteful of processor resources



- If an opponent observes *M* and MAC(*K*, *M*), it should be computationally infeasible for the opponent to construct a message *M* such that

  MAC(*K*, *M*) = MAC(*K*, *M*)

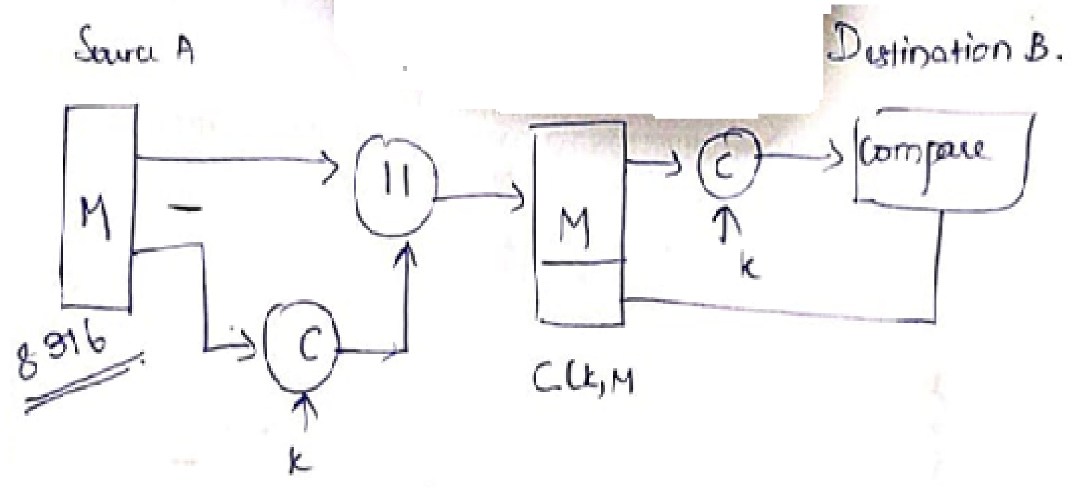
- MAC(*K*, *M*) should be uniformly distributed in the sense that for randomly chosen messages, *M* and *M*, the probability that

  MAC(*K*, *M*) = MAC(*K*, *M*)

  is 2−*n*, where *n* is the number of bits in the tag.

- Let *M* be equal to some known transformation on *M*. That is, *M* = f(*M*). For example, f may involve inverting one or more specific bits. In that case,

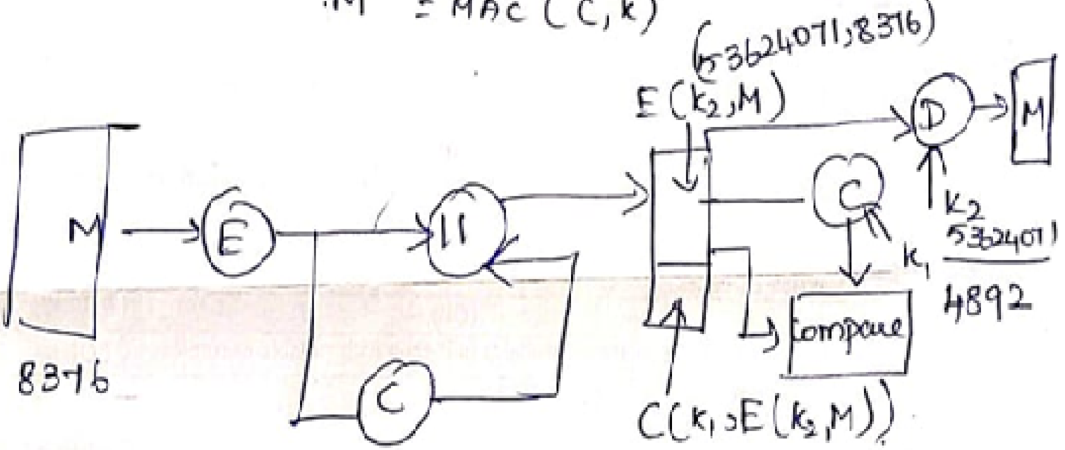
  Pr [MAC(*K*, *M*) = MAC(*K*, *M*)] = 2−*n*



$M' = MAC(M, k)$

$C = E(M, k')$

$M' = MAC(C, k)$



$M' = MAC(8376, 4892).$

$C = E(8376, 1223)$

$k' =$ prime factor of $4892 \rightarrow 1223$

$C = 312$ ... (Eulers Method).

$M' = MAC(C, k) = MAC(312, 1223)$

$\boxed{M' = 8376.} = M$

Source Message = Destination Message