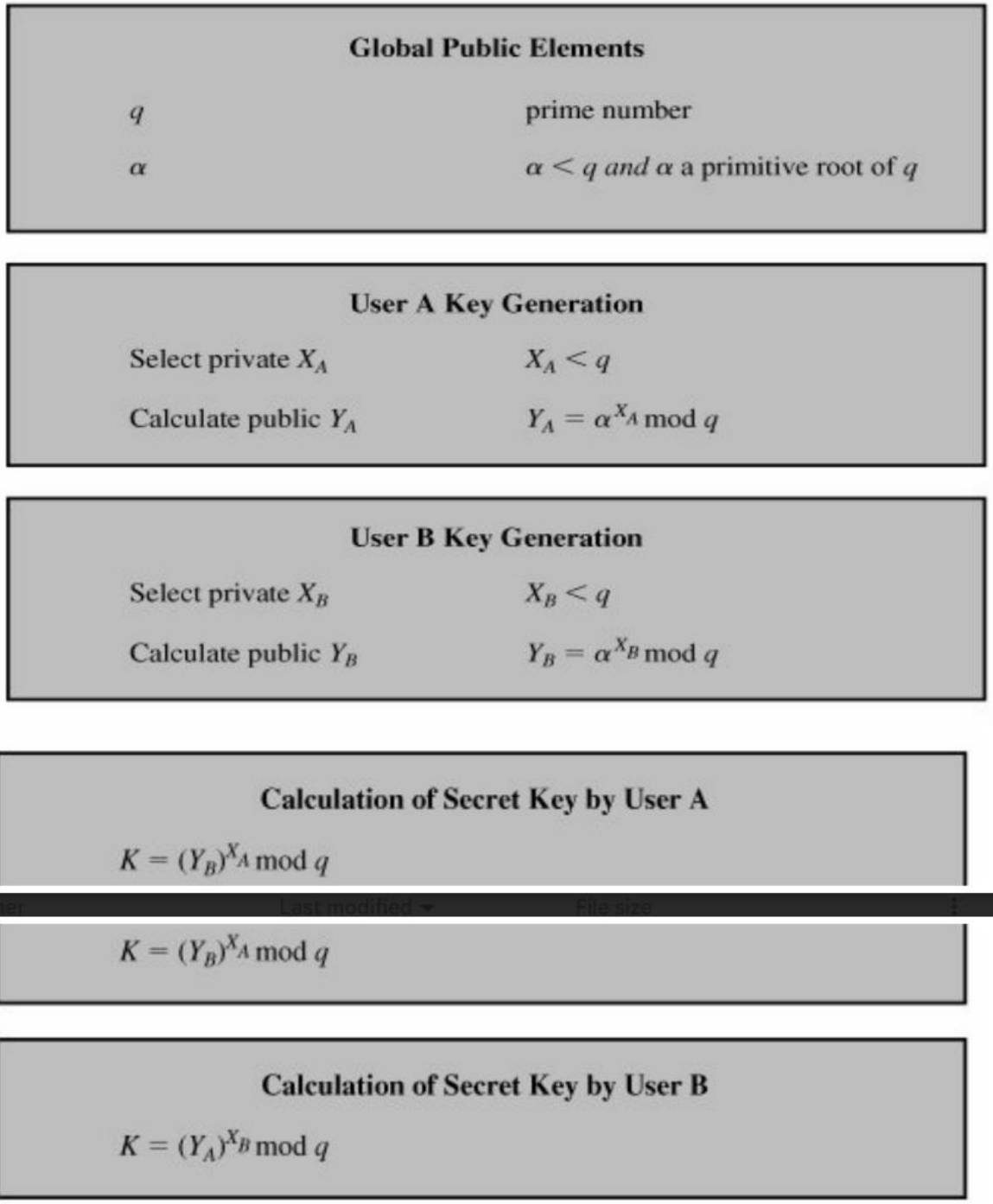
UNIT 5:

1. **Explain Diffie-Hellman key exchange.**

Ans:

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

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



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

Calculation of Secret Key by User A

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

Owner Last modified File size

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

Calculation of Secret Key by User B

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

The result is that the two sides have exchanged a secret value. Furthermore, because XA and XB are private, an adversary only has the following ingredients to work with: q, α, YA, and YB. Thus, the adversary is forced to

take a discrete logarithm to determine the key. For example, to determine the private key of user B, an adversary must compute

$$XB = \text{dlog}_{\alpha,q}(YB)$$

The adversary can then calculate the key K in the same manner as user B calculates it. The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very difficult to calculate discrete logarithms. For large primes, the latter task is considered infeasible.

2. **What is message authentication and hash function ? What types of attacks are addressed by message authentication.?**

   Or

   Discuss message authentication requirements.

Ans:

- Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent by (i.e., contain no modification, insertion, deletion, or replay) and that the purported identity of the sender is valid.

- A hash function maps a variable-length message into a fixed length hash value, or message digest. For message authentication, a secure hash function must be combined in some fashion with a secret key.

Authentication Requirements:

1. Disclosure: Release of message contents to any person or process not possessing the appropriate cryptographic key.
2. Traffic analysis: Discovery of the pattern of traffic between parties. In a connection-oriented application, the frequency and duration of connections could be determined. In either a connection-oriented or connectionless environment, the number and length of messages between parties could be determined.
3. Content modification: Changes to the contents of a message, including insertion, deletion,transposition, and modification.
4. Sequence modification: Any modification to a sequence of messages between parties,including insertion, deletion, and reordering.
5. Timing modification: Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.
6. Source repudiation: Denial of transmission of message by source.
7. Destination repudiation: Denial of receipt of message by destination.

3.What is the difference between message authentication code and hash function.?

Ans:

The following table contains the main differences between the two cryptographic primitives, Hash and MAC.

		Hash	MAC
Number of Inputs		A single input (the original message)	Two inputs (the original message + a secret key)
Output		It is called a Hash or a digest, with a fixed size	It is called a MAC or a Tag, with a size depending on the data inputs size
Algorithm		Any change in message results in a different hash	Any change in message or/and key results in a different MAC
Security goals	Confidentiality	No	No
	Integrity	Yes	Yes
	Authentication	No	Yes
Examples		SHA1, SHA2, SHA3, MD5	HMAC, CBC-MAC
Kind of keys		None	Symmetric key
Applications		Store passwords, identify files, etc	Financial cryptography, ETF, etc

4.What are the Requirements for Public-Key Cryptography.?

Ans:

1. It is computationally easy for a party B to generate a pair (public key PUb, private key PRb).
2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext:

$$C = E(PUb, M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message:

$$M = D(PRb, C) = D[PRb, E(PUb, M)]$$

4. It is computationally infeasible for an adversary, knowing the public key, PUb, to determine the private key, PRb.
5. It is computationally infeasible for an adversary, knowing the public key, PUb, and a ciphertext, C, to recover the original message, M.

We can add a sixth requirement that, although useful, is not necessary for all public-key applications:

6. The two keys can be applied in either order:

$$M = D[PUb, E(PRb, M)] = D[PRb, E(PUb, M)]$$

5.What are the principles of public key cryptosystems.?

Ans:

The concept of public-key cryptography evolved from an attempt to attack two of the most difficult problems associated with symmetric encryption.

As we have seen, key distribution under symmetric encryption requires either

(1) that two communicants already share a key, which somehow has been distributed to them; or

(2) the use of a key distribution center. Whitfield Diffie, one of the discoverers of public-key encryption (along with Martin Hellman, both at Stanford University at the time), reasoned that this second requirement negated the very essence of cryptography: the ability to maintain total secrecy over your own communication.

The second problem that Diffie pondered, and one that was apparently unrelated to the first was that of "digital signatures." If the use of cryptography was to become widespread, not just in military situations but for commercial and private purposes, then electronic messages and documents would need the equivalent of signatures used in paper documents.

6.What is the role of public and private key.?

Ans:

Private key:

In the context of encryption and decryption, a private key is a key used both for encryption and decryption. Both parties, the sender and receiver, use the private key for encryption and decryption purposes.

The encryption algorithm is the inverse of the decryption algorithm. Thus, if the encryption algorithm was created with multiplication and addition, the decryption algorithm would use division and subtraction to “break” the code.

Public key:

A public key is an encryption method that uses a pair of private and public keys to secure data communication. First, the public key encrypts the plain text, converting it into ciphertext, then the private key is used for decrypting the converted ciphertext so the recipient can read the message.

The public receives the appropriately named public key, and the receiver gets the private key. Public key cryptography is called asymmetric cryptography.

7.RSA algorithm.

Ans:

The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 21024. We examine RSA in this section in some detail, beginning with an explanation of the algorithm. Then we examine some of the computational and cryptanalytical implications of RSA.

Description of the Algorithm

The scheme developed by Rivest, Shamir, and Adleman makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to log2(n); in practice, the block size is i bits, where $2i < n\ 2i+1$. Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C:

$$C = Me \bmod n$$

$$M = Cd \bmod n = (Me)d \bmod n = Med \bmod n$$

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

1. It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all $M < n$.

2. It is relatively easy to calculate mod $M^e \bmod n$ and C^d for all values of $M < n$.

3. It is infeasible to determine d given e and n.

For now, we focus on the first requirement and consider the other questions later. We need to find a relationship of the form

$M^{ed} \bmod n = M$

The preceding relationship holds if e and d are multiplicative inverses modulo $\phi(n)$, where $\phi(n)$ is the Euler totient function. It is shown in Chapter 8 that for p, q prime, $\phi(pq) = (p\ 1)(q\ 1)$ The relationship between e and d can be expressed as

We are now ready to state the RSA scheme. The ingredients are the following:

p,q, two prime numbers (private, chosen)
n = pq (public, calculated)
e, with gcd(φ(n),e) = 1;1 < e < φ(n) (public, chosen)
d e1(mod φ(n)) (private, calculated)

8.What are the approaches to producing message authentication.?

Ans:

1. MAC
2. Hash

MAC:

An alternative authentication technique involves the use of a secret key to generate a small fixed-size block of data, known as a cryptographic checksum or MAC that is appended to the message. 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), where

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

The message plus MAC 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 MAC. The received MAC is compared to the calculated MAC .If we assume that only the receiver and the sender know the identity of the secret key, and if the received MAC matches the calculated MAC, then

1. The receiver is assured that the message has not been altered. If an attacker alters the message but does not alter the MAC, then the receiver's calculation of the MAC will differ from the received MAC. Because the attacker is assumed not to know the secret key, the attacker cannot alter the MAC 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 MAC.
3.If the message includes a sequence number (such as is used with HDLC, X.25, and TCP), then the receiver can be assured of the proper sequence because an attacker cannot successfully alter the sequence number.

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

$$h = H(M)$$

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

The hash value is appended to the message at the source at a time when the message is assumed or known to be correct. The receiver authenticates that message by recomputing the hash value. Because the hash function itself is not considered to be secret, some means is required to protect the hash value .

We begin by examining the requirements for a hash function to be used for message authentication. Because hash functions are typically quite complex, it is useful to examine some very simple hash functions to get a feel for the issues involved. We then look at several approaches to hash function design.

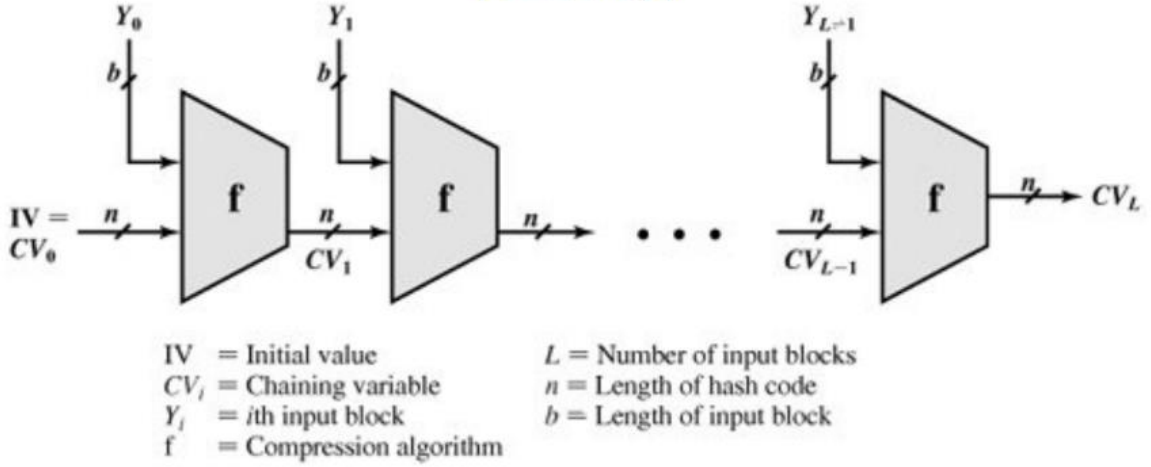
9.In what ways can a hash value be secured so as to provide message authentication.?
Ans:
There are two ways:
1.Brute Force Attacks
2.Cryptanalysis

1.Brute Force Attacks:
The strength of a hash function against brute-force attacks depends solely on the length of the hash code produced by the algorithm.In hash functions that there are three desirable properties:
- One-way: For any given code h, it is computationally infeasible to find x such that H(x) = h.
- Weak collision resistance: For any given block x, it is computationally infeasible to find y x with H(y) = H(x).
- Strong collision resistance: It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).

2.Cryptanalysis:

Figure 11.9. General Structure of Secure Hash Code

[View full size image]



The hash algorithm involves repeated use of a compression function, f, that takes two inputs (an n-bit input from the previous step, called the chaining variable, and a b-bit block) and produces an n-bit output. At the start of hashing, the chaining variable has an initial value that is specified as part of the algorithm. The final value of the chaining variable is the hash value. Often, b > n; hence the term compression. The hash function can be summarized as follows:

$$CV_0 = IV = \text{initial } n\text{-bit value}$$

$$CV_i = f(CV_{i-1}, Y_{i-1}) \quad 1 \leq i \leq L$$

$$H(M) = CV_L$$

Cryptanalysis of hash functions focuses on the internal structure of f and is based on attempts to find efficient techniques for producing collisions for a single execution of f. Once that is done, the attack must take into account the fixed value of IV. The attack on f depends on exploiting its internal structure. Typically, as with symmetric block ciphers, f consists of a series of rounds of processing, so that the attack involves analysis of the pattern of bit changes from round to round.

10.What are the essential ingredients of a public key directory.?

11.List four general categories of schemas for distribution of public keys.?