UNIT 8 DATA ENCRYPTION AND DIGITAL SIGNATURES

Structure

8.1 INTRODUCTION

One of the most powerful and important methods for security in computer systems is to encrypt sensitive records and messages in transit and in storage. Cryptography has a long and colorful history. Historically, four groups of people have used and contributed to the art of Cryptography, the military, the diplomatic corps, diarists, and lovers. The military has had the most sensitive role and has shaped the field.

At present, information and data security plays a vital role in the security of the country, the security of the corporate sector and also of every individual, working for personal benefit.

8.2 OBJECTIVES

At the end of this unit, you will able to:

- discuss what is conventional cryptography and types of ciphers;

- explain the meaning of encryptions ;
- describe Algorithms used in Cryptology;
- discuss encryption schemes, their merits and demerits;
- explain the meaning and use of Digital Signature;
- discuss cryptographic hash functions and cryptographic protocols and mechanism;
- describe methodology for ensuring the secure distribution of keys for cryptographic purposes; and
- explain the concept of trusted third parties and public key certificates.

8.3 CONVENTIONAL CRYPTOGRAPHY

The message or data to be encrypted, also known as the plaintext, is transformed by a function that is parameterized by a KEY. The output of the encryption process, known as the cipher text, is then transmitted through the insecure communication channel. The art of breaking ciphers is called cryptanalysis. The art of devising ciphers (cryptography) and breaking them (cryptanalysis) is collectively known as cryptology.

Mathematically, C = Ek (P) meaning that the encryption of the plaintext P using key K gives the cipher text C. Similarly, P = Dk(C) implies the decryption of C to get the plaintext again. It then follows that Dk (Ek (P)) = P.

8.3.1 Types of Ciphers

Conventionally, there are two types of ciphers. They are the following:

Substitution Ciphers: Another letter or group of letters to disguise it replaces each letter or group of letters. One of the oldest known ciphers is the Caesar Cipher**,** attributed to Julius Caesar. For example, using this cipher, attack becomes DWWDFN. Here plaintext is in lowercase and cipher text in uppercase letters. A slight generalisation of the Caesar cipher allows the cipher text alphabet to be shifted by k letters, instead of always 3.In this case k becomes a key to the general method of circularly shifted alphabets. Example in Fig. 1 shows:

JULIUSCAESAR Plaintext

EFGEFGEFGEFG Key EFG repeated

10 21 12 09 21 19 03 01 05 19 01 18 Plaintext, numeric

05 06 07 05 06 07 05 06 07 05 06 07 Key EFG, numeric

15 19 11 12 19 20 06 07 02 22 07 21 Cipher text (Plain XOR key)

Figure 1

A FUNCTION BASED SUBSTITUTION CIPHER

A substitution cipher can be made unbreakable by using a long no repeating key. Such a key is called one-time pad. A one-time pad may be formed by using words from a book starting from specific place known to both the sender and receiver. For example, starting with this sentence and using XOR on ASCII encoding of the letters of the plaintext and of the key. The encryption would proceed as given in Fig. 2.The textual equivalent of the cipher text is not given because it contains nonprintable ASCII characters. The message can be deciphered by reversing the process. XO Ring each letter of the cipher text with the ASCII representation of the key produces the ASCII encoding of a letter of the plaintext.

JULIUSCAESAR Plaintext

FOREXAMPLEST key-starting sentence (one-time pad)

74 85 76 73 85 83 67 65 69 83 65 82 Plaintext, ASCII

70 79 82 69 88 65 77 80 76 69 83 84 Key ASCII

12 26 30 12 13 18 14 17 09 22 18 06 Cipher text = Plain XOR key

Figure 2

A ONE-TIME PAD

One-time pad ciphers are unbreakable because they give no information to the cryptanalyst. The primary difficulty with one-time pad is that the key must be as long as the message itself, so key distribution becomes a problem, since a different pad must be used for each communication.

Transposition Ciphers: It operates by reordering the plaintext symbols, whereas substitution ciphers preserve the order of the plaintext symbols but try to disguise them. An example of it Columnar transposition is described below:

C O N S U L T   Keyword

1 4 3 5 7 2 6   Column numbers

E N C R Y P T   Plaintext:

I O N I S P E

ENCRYPTIONSPERFORMEDBYWRITINGTHEPLAINTEXT

R F O R M E D

B Y W R I T I

N G T H E P L cipher text:

A I N T E X

TEIRBNAPPETPXCNOWTNNOFYGIRIRRHTTEDILTYSMIEE

FIGURE for Transposition Cipher

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Fill in the blanks:

i) The output of the encryption process is known as ___________________.

ii) Substitution and _________________ are two types of Ciphers.

8.4 MEANING OF ENCRYPTION

Encryption is one common method of protecting information transmitted over unreliable links. In practice, the following is the mechanism of encryption:

A) The information (text) is encrypted (encoded) from its initial readable form (called clear text), to an internal form (called cipher text). This internal text form, although readable, does not make any sense.

B) The cipher text can be stored in a readable file, or transmitted over unprotected channels.

C) The receiver must decrypt (decode) it back into clear text to understand the meaning of the cipher text.

Since it is likely that people may become involved with negative aspects of computing, care has to be taken to see that encryption algorithms are free from statistical and mathematical weakness and that they are not feasible to break computationally so that cracking becomes prohibitively time-consuming. At the other end, the computational complexity of encryption and decryption should be reasonable because they represent processing overhead that increases communication delays.

8.5 ALGORITHM USED IN ENCRYPTION

The Secret-Key Algorithm: A system where one secret key shared is called Symmetric or secret key cryptography.

Data Encryption Standard (DES): It was originally developed by IBM and was adopted as an NBS Standard in 1977. It is no longer secure in its original form (Wayner, 1995), but in modified form it is still useful. DES is a symmetric cryptosystem, so the cipher text is decrypted using the same key. It operates on 64-bit (8 byte) blocks of input at a time. The algorithm, which is parameterized by a 56-bit key, has 19 distinct stages. The first stage is a key independent transposition on the 64-bit plaintext. The last stage is the exact inverse of this transposition. The stage prior to the last one exchanges the leftmost 32 bits with the rightmost 32 bits. The remaining 16 stages are functionally identical but are parameterized by different functions of the key.

The steps of the DES encryption algorithm operating on 64-bit block are:

L_0R_0 = t(input)

Repeat for n = 1 to 16

Ln = Rn–1

Rn = Ln–1 + f(Rn–1,Kn)

Output = t^{-1} (L16r16)

Obviously, DES is a complex algorithm. But critics say that its key is too short, which makes it susceptible to brute-force attack. In 1977, two standford Cryptography researchers, Diffie and Hellman designed a machine to break DES and estimated it could be built for 20 Million dollars. Given a small piece of plaintext and matched cipher text, this machine could find the key by exhaustive search of the entry key space in under 1 day. Nowadays such a machine would cost perhaps 1 million dollars. A detailed design for a machine that can break DES by exhaustive search in about four hours is presented in (Wiener, 1994).

Another calculation says that software encryption is 1000 times slower than hardware encryption and that, a high-end home computer can still do about 3, 50, 000 encryption/sec in software and is probably idle 2 million second/month. This idle time could be put to use breaking DES. Probably the most innovative idea for breaking DES is the CHINESE LOTTERY (Quisquater and Girault, 1991). With this, every radio and television has to be equipped with a cheap DES chip capable of performing 1 million encryption /sec in hardware.

Public Key Algorithms: A cryptosystem where two different keys are used for encryption and decryption is called Asymmetric or Public key System. The key distribution is the most important thing whatever may be the cryptosystem. If somehow the key is stolen, the total system would be worthless. The primary advantage of public key cryptography is increased security. The secret keys don't have to be transmitted or revealed to anyone. Another advantage of this system is that public key and the secret key can both be used for encoding as well as decoding. Their functions are interchangeable.

RSA Algorithm: These are the initials of three discoverers (Rivest, Shamir, and Adleman) at M.I.T. They all produced this algorithm, which is totally based on modular mathematics of Number theory. It is an asymmetric cryptography algorithm because it uses two different keys for encoding and decoding.

One of the properties of modular arithmetic is the possibility of computing multiplicative inverses. That is, given an integer e in the range of [0, n–1], it is sometimes possible to find a unique integer d in the range [0, n–1] such that

$$ed \bmod n = 1$$

For example, 3 and 7 are multiplicative inverses modulo 20, because 21 mod 20 = 1. It can be shown that integer e [0.n–1] has a unique multiplicative inverse mod n when e and n are relatively prime, that is when gcd (e, n) = 1.(gcd denotes the greatest common divisor). The no. of positive integers that are relatively prime to n is a function denoted as @n. For n = pq and p and q are prime, it can be shown that

$$@n = (p-1)(q-1)$$

For number P set of [0, n–1] it can be shown that the equation

$C = p^e \bmod n$ (First) is an inverse of

$P = C^d \bmod n$ (Second)

If ed mod @(n) = 1 where @n = (p–1)(q–1)

First equation is used for encryption by several public keys algorithms with e and n as the key. Decryption is performed using second equation with d and n as keys.

Since the key (e, n) is public, only the number d in the decryption pair (d, n) is private.

This above idea is used in case of RSA also. The determination of n, d and e is prescribed in the following way:

Choose two large primes, p and q, each greater than 10^{100}

Calculate n= pq and @n = (p–1)(q–1)

Assume a number d to be a large, random integer that is relatively prime to @n that is such that ed mod @(n) = 1

Calculate e such that ed mod @(n) = 1

These parameters may be used to encipher plaintext P where 0 less that equal to less than n. If the plaintext is longer, it must be broken into strings smaller than n. Cipher text is obtained as C = p^e mod n. C may be then decrypted as P = c^d mod n. Steps of algorithm ensures that encryption and decryption are inverses of each other.

Yet breaking of RSA is not reported yet wide use of it has been tremendous increased. A cryptanalyst would presumably use factoring to derive d from n and e, which are publicly known.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

Why is RSA algorithm more widely used than DES?

....

....

....

....

....

....

8.6 ENCRYPTION SCHEME: SYMMETRIC KEY VS ASYMMETRIC KEY

Symmetric-key and public-key encryption schemes have various advantages and disadvantages, some of which are common to both. This section highlights a number of these and summarizes features pointed out in previous sections.

i) Advantages of symmetric-key cryptography

1) Symmetric-key ciphers can be designed to have high rates of data throughput. Some hardware implementations achieve of hundreds of megabytes per second, while software implementations may attain throughput rates in the megabytes per second range.

2) Keys for symmetric-key ciphers are relatively short.

3) Symmetric-key ciphers can be employed as primitives to construct various cryptographic mechanisms including pseudorandom number generators, hash functions and computationally efficient digital signature schemes, to name just a few.

4) Symmetric-key ciphers can be composed to produce stronger ciphers. Simple transformations which are easy to analyse, but are weak on their own weak, can be used to construct strong product ciphers.

5) Symmetric-key encryption is perceived to have an extensive history, although it must be acknowledged that, notwithstanding the invention of rotor machines earlier, much of the knowledge in this area has been acquired subsequent to the invention of the digital computer, and in particular, the design of the Data Encryption Standard in the early 1970s.

ii) Disadvantages of symmetric-key cryptography

1) In a two-party communication, the key must remain secret at both ends.

2) In a large network, there are many key pairs to be managed. Consequently, effective key management requires the use of an unconditionally trusted TTP .

3) In a two-party communication between entities µ and ¶, sound cryptographic practice dictates that the key be changed frequently and perhaps for each communication session.

4) Digital signature mechanisms arising from symmetric-key encryption typically require either large keys for the public verification function or the use of a TTP.

iii) Advantages of public-key cryptography

1) Only the private key must be kept secret (authenticity of public keys must, however, be guaranteed).

2) The administration of keys on a network requires the presence of only a functionally trusted TTP as opposed to an unconditionally trusted TTP. Depending on the mode of usage, the TTP might only be required in an “off-line” manner, as opposed to in real time.

3) Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable periods of time, e.g., many sessions (even several years).

4) Many public-key schemes yield relatively efficient digital signature mechanisms. The key used to describe the public verification function is typically much smaller than for the symmetric-key counterpart.

5) In a large network, the number of keys necessary may be considerably smaller than in the symmetric-key scenario.

iv) Disadvantages of public-key encryption

1) Throughput rates for the most popular public-key encryption methods

are several orders of magnitude slower than the best-known symmetric-key schemes.

2) Key sizes are typically much larger than those required for symmetric-key encryption and the size of public-key signatures is larger than that of tags providing data origin authentication from symmetric-key techniques.

3) No public-key scheme has been proven to be secure (the same can be said for block ciphers). The most effective public-key encryption schemes found to date have their security based on the presumed difficulty of a small set of number-theoretic problems.

4) Public-key cryptography does not have as extensive a history as symmetric-key encryption, being discovered only in the mid 1970s.

Summary of comparison

Symmetric-key and public-key encryptions have a number of complementary advantages.

Current cryptographic systems exploit the strengths of each. Public-key encryption techniques may be used to establish a key for a symmetric-key system being used by communicating entities and in this scenario, we can take advantage of the long term nature of the public/private keys of the public-key scheme and the performance efficiencies of the symmetric-key scheme. Since data encryption is frequently the most time consuming part of the encryption process, the public-key scheme for key establishment is a small fraction of the total encryption process.

To date, the computational performance of public-key encryption is inferior to that of symmetric-key encryption. There is, however, no proof that this must be the case. The important points in practice are:

1. Public-key cryptography facilitates efficient signatures (particularly non-repudiation) and key management; and

2. Symmetric-key cryptography is efficient for encryption and some data integrity applications.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

What are the basic advantages of Asymmetric Key?

....

....

....

....

....

....

8.7 DIGITAL SIGNATURE

People authenticate other people by recognising their faces, voices and handwriting. Signatures on letterhead paper handle proof of signing raised seals and so on. Handwriting, paper, and ink experts can usually detect tampering. But none of these options are available electronically. That's why the concept of Digital signature came into existence to authenticate electronic documents.

A Digital Signature is a technique by which it is possible to secure electronic information in such a way that the originator of the information, as well as the integrity of the information, can be verified. This procedure of guaranteeing the origin and the integrity of the information is also called Authentication.

The authenticity of many legal, financial, and other documents is determined by the presence or absence of an authorized handwritten signature. For a computerised message system to replace the physical transport of paper and ink documents handwritten signatures have to be replaced by Digital Signatures. Basically what is needed, is a system by which one party can send a "signed" message to another party in such a way that

A) The receiver can verify the claimed identity of the sender.

B) The sender cannot repudiate the contents of the message.

C) The receiver cannot possibly have concocted the message himself/ herself.

A digital signature is only a technique that can be used for different authentication purposes. For an E-record, it comes functionally very close to the traditional hand-written signatures. The user himself/ herself can generate key pair by using specific crypto software. Now Microsoft IE and Netscape, allow the user to create his/ her own key pair.

Here, the most important thing is how can the user be sure that public keys belong to his/ her partner only? In this case, a third party (TTP) will guarantee the relationship between the identity and the public keys. The TTP are popularly called Certified Authorities (CAs).

Digital Certificate: These certificates are provided by CAs to authenticate that a particular site is globally secured. There are so many reputed CAs all over the world. Some of them are Very Sign from USA and Thawte Consulting from South Africa. Popular India CAs are SafeScrypt Ltd, TCS, IDRBT, MTNL Ltd and NIC.

Digital certificates contain the following:

Issuer, Issued to, orgnization name, organization unit, validity, Version, Public Keys, Thumbprint, algorithms etc.

Secure Socket Layer (SSL) is the widely used protocol for digital certificates. The Uniform Resource Locator (URL) starts with "https" instead of "http" and are secured by SSL. At the bottom of the window, a lock symbol appears for SSL. Generally 128 bits SSL are used.40 bits SSL are also available.

Please answer the following Self Assessment Question.

Self Assessment Question 4 *Spend 3 Min.*

Is digital signature equivalent to handwritten signature legally?

....

....

....

....

8.8 AUTHENTICATION AND IDENTIFICATION

Authentication is a term which is used (and often abused) in a very broad sense. By itself, it has little meaning other than to convey the idea that some means has been provided to guarantee that entities are who they claim to be, or that information has not been manipulated by unauthorized parties. Authentication is specific to the security objective which one is trying to achieve. Examples of specific objectives include access control. The host countries might not permit secrecy on the channel; one or both countries might want the ability to monitor all communications. Jack and Bond, however, would like to be assured of the identity of each other, and of the integrity and origin of the information they send and receive.

Authentication is one of the most important of all information security objectives. Until the mid 1970s it was generally believed that secrecy and authentication were intrinsically connected. With the discovery of hash functions and digital signatures, it was realised that secrecy and authentication were truly separate and independent information security objectives. It may at first not seem important to separate the two but there are situations where it is not only useful but essential. For example, if a two-party communication between Jack and Bond is to take place where Jack is in one country and Bond in another, the host countries might not permit secrecy on the channel; one or both countries might want the ability to monitor all communications. Jack and Bond, however, would like to be assured of the identity of each other, and of the integrity and origin of the information they send and receive.

The preceding scenario illustrates several independent aspects of authentication. If Jack and Bond desire assurance of each other's identity, there are two possibilities to consider.

1) Jack and Bond could be communicating with no appreciable time delay. That is, they are both active in the communication in "real time".

2) Jack or Bond could be exchanging messages with some delay. That is, messages might be routed through various networks, stored, and forwarded at some later time. In the first instance Jack and Bond would want to verify identities in real time. This might be accomplished by Jack sending Bond some challenge, to which Bond is the only entity which can respond correctly. Bond could perform a similar action to identify Jack. This type of authentication is commonly referred to as *entity authentication* or more simply phrase challenge for *identification*.

For the second possibility, it is not convenient to challenge and await response, and moreover the communication path may be only in one direction. Different techniques are now required to authenticate the originator of the message. This form of authentication is called *data origin authentication*.

Thus *Data origin authentication* or *message authentication* techniques provide to one for originality.

8.9 HASH FUNCTIONS

One of the fundamental primitives in modern cryptography is the cryptographic hash function, often informally called a one-way hash function simplified definition of hash function is given below.

Definition A *hash function* is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length, called *hash-values*.

The most common cryptographic uses of hash functions are with digital signatures and for data integrity. With digital signatures, a long message is usually hashed (using a publicly available hash function) and only the hash-value is signed. The party receiving the message then hashes the received message and verifies that the received signature is correct for this hash-value. This saves both time and space compared to signing the message directly, which would typically involve splitting the message into appropriate-sized blocks and signing each block individually. Note here that the inability to find two messages with the same hash-value is a security requirement, since otherwise, the signature on one message hash-value would be the same as that on another, allowing a signer to sign one message and at a later point in time claim to have signed another.

Hash functions may be used for data integrity as follows. The hash-value corresponding to a particular input is computed at some point in time. The integrity of this hash-value is protected in some manner. At a subsequent point in time, to verify that the input data has not been altered, the hash-value is recomputed using the input at hand, and compared for equality with the original hash-value. Specific applications include virus protection and software distribution.

A third application of hash functions is their use in protocols involving prior commitments, including some digital signature schemes and identification protocols.

Hash functions as discussed above are typically publicly known and involve no secret keys. When used to detect whether the message input has been altered, they are called *modification detection codes* (MDCs). Related to these are hash functions which involve a secret key, and provide data origin authentication as well as data integrity; these are called *message authentication codes* (MACs).

8.10 PROTOCOL AND MECHANISMS

Definition A *cryptographic protocol* (*protocol*) is a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective.

Remark (*protocol vs mechanism*) As opposed to a protocol, a *mechanism* is a more general term encompassing protocols, algorithms (specifying the steps followed by a single entity), and non-cryptographic techniques (e.g., hardware protection and procedural controls) to achieve specific security objectives.

Protocols play a major role in cryptography and are essential in meeting cryptographic goals. Encryption schemes, digital signatures, hash functions, and random number generation are among the primitives which may be utilized to build a protocol.

Protocol and mechanism failure

Definition A *protocol failure* or *mechanism failure* occurs when a mechanism fails to meet the goals for which it was intended, in a manner whereby an adversary gains advantage not by breaking an underlying primitive such as an encryption algorithm directly, but by manipulating the protocol or mechanism itself.

Example (*mechanism failure*) Jack and Bond are communicating using a stream cipher.

Messages which they encrypt are known to have a special form: the first twenty bits carry information which represents a monetary amount. An active adversary can simply XOR an appropriate bit string into the first twenty bits of cipher text and change the amount. While the adversary has not been able to read the underlying message, she has been able to alter the transmission. The encryption has not been compromised but the protocol has failed to perform adequately; the inherent assumption that encryption provides data integrity is incorrect.

Example (*forward search attack*) Suppose that in an electronic bank transaction the bit field which records the value of the transaction is to be encrypted using a public-key scheme. This simple protocol is intended to provide privacy of the value field – but does it? An adversary could easily take all possible entries that could be plaintext in this field and encrypt them using the public encryption function. (Remember that by the very nature of public-key encryption this function must be available to the adversary.) each of the cipher texts with the one which is actually encrypted in the transaction, the adversary can determine the plaintext. Here the public-key encryption function is not compromised, but rather the way it is used.

8.11 KEY ESTABLISHMENT, MANAGEMENT AND CERTIFICATION

This section gives a brief introduction to methodology for ensuring the secure distribution of keys for cryptographic purposes.

Definition *Key establishment* is any process whereby a shared secret key becomes available to two or more parties, for subsequent cryptographic use.

Definition *Key management* is the set of processes and mechanisms which support key establishment and the maintenance of ongoing keying relationships between authorized parties, including replacing older keys with new keys as and when necessary.

Key establishment can be broadly subdivided into *key agreement* and *key transport*. Many and protocols have been proposed to provide key establishment.

Key management encompasses techniques and procedures supporting:

1. initialisation of system users within a domain;
2. generation, distribution, and installation of keying material;

3. controlling the use of keying material;

4. update, revocation, and destruction of keying material; and

5. storage, backup/recovery, and archival of keying material.

Key management through symmetric-key techniques

One solution which employs symmetric-key techniques involves an entity in the network which is trusted by all other entities. This entity is referred to as a *trusted third party* (TTP). Each entity shares a distinct symmetric key with the TTP. These keys are assumed to have been distributed over a secured channel. If two entities subsequently wish to communicate, the TTP generates a key (sometimes called a *session key*) and sends it encrypted under each of the fixed keys. This approach has certain advantages and disadvantages.

A symmetric cryptographic system is a system involving two transformations – one for the originator and one for the recipient – both of which make use of either the same secret key (symmetric key) or two keys easily computed from each other. An asymmetric cryptographic system is a system involving two related transformations – one defined by a public key (the public transformation), and another defined by a private key (the private transformation) – with the property that it is computationally infeasible to determine the private transformation from the public transformation.

Advantages

1. It is easy to add and remove entities from the network.

2. Each entity needs to store only one long-term secret key.

Disadvantages

1. All communications require initial interaction with the TTP.

2. The TTP must store long-term secret keys.

3. The TTP has the ability to read all messages.

4. If the TTP is compromised, all communications are insecure.

Key management through public-key techniques

There are a number of ways to address the key management problem through public-key techniques. Each entity in the network has a public/private encryption key pair. The public key along with the identity of the entity is stored in a central repository called a *public file*.

Advantages of this approach include:

1. No trusted third party is required.

2. The public file could reside with each entity.

3. Only public keys need to be stored to allow secure communications between any pair of entities, assuming the only attack is that by a passive adversary.

The key management problem becomes more difficult when one must take into account an adversary who is *active* (i.e. an adversary who can alter the public file containing public keys).

Please answer the following Self Assessment Question.

Self Assessment Question 5 *Spend 1 Min.*

Key establishment can be divided into ____________________ and key transport.

8.12 TRUSTED THIRD PARTIES AND PUBLIC KEY CERTIFICATES

Definition A TTP is said to be *unconditionally trusted* if it is trusted on all matters. For example, it may have access to the secret and private keys of users, as well as be charged with the association of public keys to identifiers.

Various third party services require different types of trust and competency in the third party. For example, a third party possessing secret decryption keys (or entity authentication keys) must be trusted not to disclose encrypted information (or impersonate users). A third party required (only) to bind an encryption public key to an identity must still be trusted not to create false associations and thereafter impersonate an entity. In general, three levels of trust in a third party T responsible for certifying credentials for users may be distinguished. Level 1: T knows each user's secret key. Level 2: T does not know users' secret keys, but can create false credentials without detection. Level 3: T does not know users' secret keys, and generation of false credentials is detectable

Definition A TTP is said to be *functionally trusted* if the entity is assumed to be honest and fair but it does not have access to the secret or private keys of users.

Public-key certificates

The distribution of public keys is generally easier than that of symmetric keys, since secrecy is not required. However, the integrity (authenticity) of public keys is critical.

Primary advantages offered by public-key (vs symmetric-key) techniques for applications related to key management include:

1) *Simplified key management*. To encrypt data for another party, only the encryption public key of that party need be obtained. This simplifies key management as only authenticity of public keys is required, not their secrecy. . The situation is analogous for other types of public-key pairs, e.g., signature key pairs.

2) *On-line trusted server not required*. Public-key techniques allow a trusted on-line server to be replaced by a trusted off-line server plus any means for delivering authentic public keys (e.g., public-key certificates and a public database provided by an un-trusted on-line server). For applications where an on-line trusted server is not mandatory, this may make the system more amenable to scaling, to support very large numbers of users.

3) *Enhanced functionality*. Public-key cryptography offers functionality which typically cannot be provided cost-effectively by symmetric techniques (without additional online trusted third parties or customized secure

hardware). The most notable such features are non-repudiation of digital signatures, and true (single-source) data origin authentication.

A *public-key certificate* consists of a *data part* and a *signature part*. The data part consists of the name of an entity, the public key corresponding to that entity, possibly additional relevant information (e.g., the entity's street or network address, a validity period for the public key, and various other attributes). The signature part consists of the signature of a TTP over the data part.

8.13 PSEUDORANDOM NUMBERS AND SEQUENCES

Random number generation is an important primitive in many cryptographic mechanisms.

For example, keys for encryption transformations need to be generated in a manner which is unpredictable to an adversary. Generating a random key typically involves the selection of random numbers or bit sequences. Random number generation presents challenging issues.

Often in cryptographic applications, one of the following steps must be performed:

i) From a finite set of elements, select an element at random.

ii) From the set of all sequences (strings) of length over some finite alphabet of symbols, select a sequence at random.

iii) Generate a random sequence (string) of symbols of length over a set of symbols.

It is not clear what exactly it means to select at random or generate at random. Calling a number random without a context makes little sense. Is the number a random number?

Let us now summarize the points covered in this unit.

8.14 SUMMARY

- Encryption is one common method of protecting information transmitted over unreliable lines where plain text is being converted to Cipher text and then again to plain text.

- Basically there are two algorithms used for encryption .One is RSA and other one is DES.

- RSA is an asymmetric cryptography and DES is symmetric one.

- A system where one secret key shared is called Symmetric or Secret Key Cryptography.

- A cryptosystem where two different keys are used for encryption and decryption is called Asymmetric or Public Key System.

- Digital signature is a technique to secure electronic information in such a way that the originator of the information, as well as the integrity of information can be verified with proper authentication.

- Digital certificates are provided by Certified Authorities (CAs) to authenticate that a particular site is globally secured.
- There are five common CAs in India. They are Safescrypt Ltd, TCS, IDRBT, MTNL and NIC.
- A hash function is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length called hash-values. The most common cryptographic uses of hash functions are with digital signatures and for data integrity.
- Key establishment is any process whereby a shared secret key becomes available to two or more parties, for subsequent cryptographic use.
- Key establishment can be subdivided into key agreement and key transport.
- Key management is the set of processes and mechanisms, which support key establishment and the maintenance of ongoing keying relationships between parties, including replacing older keys with new keys as and when necessary.

8.15 TERMINAL QUESTIONS

1) What do you mean by Encryption? Describe RSA algorithm with examples.

2) How do you know that URL is secured?

3) What are the differences between digital signatures and certificates?

8.16 ANSWERS AND HINTS

Self Assessment Questions

1) (i) Cipher text, (ii) Transposition

2) RSA is asymmetric cryptographic algorithm and uses two different keys for encoding and decoding while DES is a symmetric cryptosystem and the cipher text is decrypted using the same key. It is a complex algorithm. So far no breaking of RSA has been reported though DES can be broken.

3) The advantages of Asymmetric keys are as follows:

   1) Only the private key must be kept secret

   2) The administration of keys on a network requires the presence of only a functionally trusted TTP as opposed to an unconditionally trusted TTP

   3) Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable periods of time.

4) According to Patrick W. Brown, Digital Signature technology may be employed to produce legally enforceable signatures in Electronic Data Interchange (EDI) among computer users within the same general guidelines and requirements as those developed for handwritten signatures on paper. Digital Signature technology may be employed to produce legally enforceable signatures in Electronic Data Interchange (EDI) among computer users within the same general guidelines and requirements as technology promises assurance at least

equal to written signatures. From a legal standpoint, this assurance remains to be tested in the evidentiary process. Business policies for organizational use of this technology are being created as the use of digital signature technology is adopted. Digital signatures may be used to provide assurances in distributed and networked computer environments where electronic transactions require a high degree of trust.

5) Key Agreement

Terminal Questions

1) Refer to section 8.4 and 8.5 of the unit.

2) Refer to section8.7 of the unit.

3) Refer to section 8.7 and 8.13 of the unit.

Apart from above, please follow other reference books for in depth knowledge.

8.17 REFERENCES AND SUGGESTED READINGS

1. Brown, P.W. "Digital signatures: are they legal for electronic commerce". Communications Magazine. IEEE. 32.9 (Sept. 1994): 76 – 80.

2. Mlen Milenkivic. Operating System Concepts and design. New York : McGraw-Hill, Inc, 1992.

3. Silberschatz. Galvin, Gagne. Operating System Concepts. 7th ed. John Wiley & Sons, 2006.