Chapter 5

Network Security

LEARNING OBJECTIVES

- *Network security basics*
- *Terminologies*
- *Cryptographic techniques*
- *Encryptions*
- *Types of keys*
- *Traditional cipher algorithms*
- *Substitution cipher*
- *Traditional cipher*
- *Symmetric key encryption*
- *Asymmetric key encryption*
- *Diffie-hellman*
- *Digital signatures and certificates*

Network Security Basics

It is necessary to define some fundamental terms relating to network security and are the elements used to measure the security of a network. These terms are used to measure the security of a network. To be considered sufficiently advanced along the spectrum of security, a system must adequately address identification, integrity, accountability, non-repudiation, authentication, availability, confidentiality each of which is defined in the following sections:

Identification

Identification is simply the process of identifying one's self to another entity or determining the identity of the individual or entity, with whom you are communicating.

Authentication

Authentication serves as proof that you are who you say you are or what you claim to be. Authentication is critical if there is to be any trust between parties. Authentication is required when communicating over a network or logging into a network. When communicating over a network you should ask yourself two questions.

1. With whom am I communicating?
2. Why do I believe this person or entity is who he claims to be?

Access Control (Authorization)

This refers to the ability to control the level of access that individuals or entities have to a network or system and how much information they can receive. Level of authorization basically determines what you're allowed to do once you are authenticated and allowed access to a network, system or some other resource such as data or information. Access control is the determination of the level of authorization to a system, network or information.

Availability

This refers to whether the network, system, hardware and software are reliable and can recover quickly and completely in the event of an interruption in service. Ideally, these elements should not be susceptible to denial of service attacks.

Confidentiality

This is also be called privacy or secracy to the protection of information from unauthorized disclosure. Usually achieved either by restricting access to the information or by encrypting the information so that it is not meaningful to unauthorized individuals or entities.

Integrity

This can be thought of as accuracy, this refers to the ability to protect information, data, or transmissions from unauthorized, uncontrolled, or accidental alterations.

Accountability

This refers to the ability to track or audit what an individual or entity is doing on a network or system.

Non-repudiation

The ability to prevent individuals or entities from denying (repudiating) that information, data or files were sent or received or that information or files were accessed or altered, when infact they were. This capability is crucial in e-commerce, without if an individual or

entity can deny that he, she or it is responsible for a transaction and that he, she or it is, therefore, not financially liable.

Threats

A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system. This can take any form and can be malevolent, accidental, or simply an act of nature.

Vulnerabilities

A vulnerability is an inherent weakness in the design, configuration, implementation, or management of a network or system that renders it susceptible to a threat. Vulnerabilities are what make networks susceptible to information loss and downtime. Every network and system has some kind of vulnerability.

Attacks

An attack is a specific technique used to exploit a vulnerability. For example, a threat could be a denial of service. A vulnerability is in the design of the operating system, and an attack could be a 'Ping of death'. There are two general categories of attacks:

1. Passive
2. Active

Passive attacks These are very difficult to detect because there is no overt activity that can be monitored or detected.

Examples of passive attacks would be packet sniffing or traffic analysis.

These types of attacks are designed to monitor and record traffic on the network. They are usually employed for gathering information that can be used later in active attacks.

Active attacks These employ more overt actions on the network or system. As a result, they can be easier to detect, but at the same time they can be much more devastating to a network.

Examples of this type of attack would be a denial-of-service attack or active probing of systems and networks.

Viruses

A virus, a parasitic program that cannot function independently, is a program or code fragment that is self propagating. It is called a virus, because like its biological counterpart, it requires a 'host' to function. In the case of a computer virus the host is some other program to which the virus attaches itself. A virus is usually spread by executing an infected program or by sending an infected file to someone else, usually in the form of an e-mail attachment.

Worm

A worm is a self-contained and independent program that is usually designed to propagate or spawn itself on infected systems and to seek other systems via available networks. The difference between a virus and a Worm is that a virus is not an independent program.

Trojan horses

A trojan horse is a program or code fragment that hides inside a program and performs a disguised function. A trojan horse program hides within another program or disguises itself as a legitimate program. This can be accomplished by modifying the existing program or by simply replacing the existing program with a new one. The Trojan horse program functions much the same way as the legitimate program, but usually it also performs some other function, such a recording sensitive information or providing a trap door. An example would be a 'password grabber'.

Logic bombs

A logic bomb is a program or subsection of a program designed with malevolent intent. It is referred to as a logic bomb, because the program is triggered when certain logical conditions are met. This type of attack is almost always perpetrated by an insider with privileged access to the network. The perpetrator could be a programmer or a vendor that supplies software.

Denial of service (DOS)

Denial of service attacks are designed to shut down or render inoperable a system or network. The goal of the denial-of-service attack is not to gain access or information but to make a network or system unavailable for use by other users. It is called denial-of-service attack, because the end result is to deny legitimate users access to network services.

Protection against network threats

Network threats may cause a massive harm to the system, as the network users are increasing, there is a good chance to attack a system protection against threats should be done.

To protect system form virus and worms, a security suite should be installed.

Similarly, to protect a system from Trojan horse, internet security suite prevents from downloading Trojan horse.

SPAM filters should be used to stop SPAM, this is available within the mail servers by default.

A strong encryption should be used to protect against packet sniffers, so that packets become unreadable making packet sniffers useless.

Cryptographic Techniques

For the exchange of information and commerce to be secure on any network, a system or process must be put in place that satisfies requirements for confidentiality, access control, authentication, integrity, and non-repudiation. The key

to the securing information on a network is cryptography. Cryptography can be used as a tool to provide privacy.

Traditionally, cryptography conjures up thoughts of spies and secret codes. In reality, cryptography and encryption have found broad applications in society. Every time you use an ATM machine to get cash or a point-of-sale machine to make a purchase, you are using encryption.

Encryption

Encryption is the process of scrambling the contents of a file or message to make it unintelligible to anyone not in possession of the 'key' required to unscramble it.

A cryptosystem or algorithm is the process or procedure to turn plain text into crypto text. A crypto algorithm is also known as a 'cipher'. Theoretically, all algorithms can be broken by one method or another. However, an algorithm should not contain an inherent weakness that an attacker can easily exploit

Example: Below is an example of a cipher, to scramble a message with this cipher, simply match each letter in a message to the first row and convert it into the number or letter in the second row. To unscramble a message, match each letter or number in a message to the corresponding number or letter in the second row and convert it into the letter in the first row.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

To illustrate how this works see the following where the cipher is used to scramble the message:

'Little green apples'

Cipher text: FCNNF5 AL55H 1JJF5M
Clear text: LITTLE GREEN APPLES

This cipher would not be effective at keeping a message secret for long. It does not comply with one of the qualities of a truly effective cipher. Ciphers usually fall into one to two categories:

1. Block Ciphers
2. Stream Cipher

Stream ciphers

Steam cipher algorithms process plaintext to produce a stream of cipher text. The cipher inputs the plaintext in a stream and outputs a steam of cipher text.

Example:
Plaintext: LET US TALK ONE TO ONE
Cipher text: F5N OM NLFE ITS NI ITS

Stream cipher have several weaknesses. The most crucial short coming of stream ciphers is the fact that patterns in the plain text can be reflected in the cipher text. Knowing that certain words repeat makes breaking the code easier. In addition, certain words in the English language appear with predictable regularity. Letters of the alphabet also appear in predictable regularity. The most commonly used letters of the alphabet in the English language are E, T, A, O, N and I. The least commonly used letters are J, K, X, Q and Z. The most common combination of letters in the English language is '*th*', As a result, if a code breaker is able to find a '*t*' in a code, it doesn't take long to find an '*h*'.

Block ciphers

Block ciphers differ from stream ciphers in that they encrypt and decrypt information in fixed size blocks rather than encrypting and decrypting each letter or word individually. A block cipher passes a block of data or plaintext through its algorithm to generate a block of cipher text. Another requirement of block cipher is that the cipher texts should contain no detectable pattern.

Types of keys

We deal with three types of keys in cryptography:

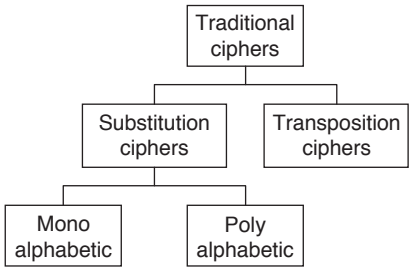
1. Secret key
2. Public key
3. Private Key

- The secret key, is the shared key used in symmetric-key cryptography.
- Public and Private keys are used in asymmetric-key cryptography.
- In symmetric-key cryptography, the same key locks and unlocks the box.
- In asymmetric-key cryptography, one key locks the box, but another key is needed to unlock it.

Traditional Cipher Algorithms

Traditional ciphers are character oriented, these ciphers can be divided into two broad categories:

1. Substitution ciphers
2. Transposition ciphers.



Substitution Cipher

A substitution cipher substitutes one symbol with another. If the symbols in the plain text are alphabetic characters, we replace one character with another. Substitution ciphers can be categorized as either mono-alphabetic or poly-alphabetic ciphers.

- In a mono-alphabetic cipher, a character or symbol in the plaintext is always changed to the same character or symbol in the cipher text regardless of its position in the text. For example if the algorithm says that character '*A*' in the plain text is changed to character '*E*', every character '*A*' is changed to character '*E*'.
- The relationship between characters in the plain text and the cipher text is a one-to-one relationship.
- In a poly-alphabetic cipher, each occurrence of a character can have a different substitute. The relationship between a character in the plain text to a character in the cipher text is a one-to-many relationship.
- To achieve this goal, we need to divide the text into groups of characters and use a set of keys.
- In substitution cipher, if 'a' becomes *D*, '*b*' becomes '*E*' then the word 'corrupt' becomes ETUUXSW, plain text will be given in lower case, and cipher text in upper case.
- A slight generalization of the ceasar cipher allows the cipher text alphabet to be shifted by '*K*' letters, instead of always '3'.
- The next improvement is to have each of the symbols in the plain text, say, the 26 letter for simplicity, map onto some other letter.

Example:

Plain Text	a	b	c	d	e	f	g	h	i	j
Cipher Text	L	N	O	B	R	M	S	U	V	Z

Plain text	k	l	m	n	o	p	q	r	s	t	u
Cipher Text	P	A	K	C	L	H	W	Q	X	Y	J

Plain Text	v	w	x	y	z
Cipher Text	E	F	D	G	J

Plain Text	corrupt
Cipher Text	OIQQJHY

- In this method, if a small cipher is given it can be broken easily. The basic attack takes advantage of the statistical properties of natural languages. For example, In English, '*e*' is the most common letter followed by *t*, *o*, *a*, *n*, *i* etc.
- The most common 2 letter combinations, are *th*, *in*, *er*, *re* and *an*.
- The most common three-letter combinations are are, the, ing, and, and ion.
- By making guesses at common letters, digrams and trigrams and knowing about likely patterns of vowels and consonants, the cryptanalyst builds up a tentative plaintext, letter by letter.

Transposition Ciphers

Substitution ciphers preserve the order of the plaintext symbols but disguise them.

Transposition ciphers, in contrast, reorder the letters but do not disguise them. Following figure depicts a common transposition cipher, the columnar transposition.

- The cipher is keyed by a word or phrase not containing any repeated letters.

Example: 'NETWORKS' is the key.
Plaintext: Transfer ten million dollars to my account.
What is the cipher text using transposition cipher?

Solution: Key: NETWORKS

N	E	T	W	O	R	K	S
3	1	7	8	4	5	2	6
T	r	a	n	s	f	e	r
t	e	n	m	i	l	l	i
o	n	d	o	l	l	a	r
s	t	o	m	y	a	c	c
o	u	n	t	a	b	c	d

The purpose of key is to number the columns, column 1 being under the key letter closest to the start of the alphabet, and so on.

The plain text is written horizontally in rows, padding is required to fill the matrix, if it is not complete'. The cipher text is read out by columns, starting with the column whose key letter is the lowest.

Plain text: Transfer ten million dollars to my account
Cipher Text: rentue laccttososilyafllabrircdandonnmomt.

Symmetric Key Encryption

Symmetric key, also referred to as private key or secret key, is based on a single key and algorithm being shared between the parties who are exchanging encrypted information. The same key both encrypts and decrypts messages.

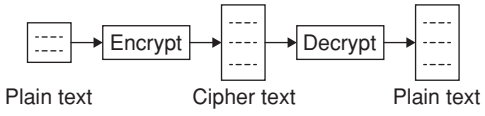


Figure 1 Symmetric key encryption

The strength of the scheme is largely dependent on the size of the key and on keeping it secret. Generally the larger the key, the more secure the scheme. In addition, symmetric key encryption is relatively fast. Private key cryptosystems are not well suited for spontaneous communication over open and unsecured networks. Symmetric key provides on process for authentication or non-repudiation.

Data Encryption Standard: (DES)

DES consists of an algorithm and a key. The key is a sequence of eight bytes, each containing eight bits for a 64 bit key. Since each byte contains one parity bit, the key is actually 56 bits in length. DES is widely used in automated teller machine (ATM) and point-of-sale (POS) networks, so if you use an ATM or debit card you are using DES.

Asymmetric Key Encryption

Asymmetric cryptography is also known as public key cryptography, public key cryptography uses two keys one is public key and the other is private key. The key names describe their function. One key is kept private, and the other key is made public. Knowing the public key doesn't reveal the private key. A message encrypted by the private key can only be decrypted by the corresponding public key. Conversely, a message encrypted by the public key can only be decrypted by the private key.

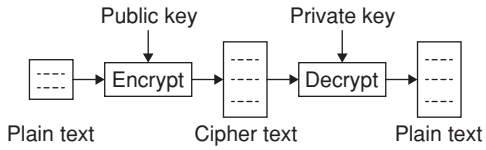


Figure 2 Asymmetric key encryption

With the aid of public key cryptography, it is possible to establish secure communications with any individual or entity when using a compatible software or hardware device.

There are three public key algorithms in wide use today:

1. Diffie–Hellman
2. RSA
3. Digital Signature Algorithm (DSA)

Diffie–Hellman

It was the first usable public key algorithm. Diffie–Hellman is based on the difficulty of computing discrete logarithms. It can be used to establish a shared secret key that can be used by two parties for symmetric encryption. Diffie–Hellman is often used for IPsec key management protocols. For spontaneous communications with Diffie–Hellman, two communicating entities would each generate a random number that is used as their private keys. They exchange public keys they each apply their private keys to the other's. public key to compute identical values (shared secret key). They then use the shared secret key to encrypt and exchange information.

Diffie–Hellman key exchange

The protocol that allows strangers to establish a shared secret key is called the Diffie–Hellman key exchange and works as follows:

- Ana and Brat have to agree on 2 large numbers, 'n' and 'g', where 'n' is a prime.
- $(n-1)/2$ is also a prime and certain conditions apply to 'g'.
- These numbers may be public, so either one of them can just pick 'n' and 'g' and tell the other openly.
- Now Ana picks a large number (suppose 512-bit) 'x', and keeps it secret. Similarly Brat picks a large secret number, 'y'.
- Ana initiates the key exchange protocol by sending Brat a message containing $(n, g, g^x \bmod n)$
- Brat responds by sending Ana a message containing $(g^y \bmod n)$
- Now Ana raises the number Brat sent her to the xth power modulo 'n' to get $[(g^y \bmod n)^x \bmod n]$
- Brat performs a similar operation to get $[(g^x \bmod n)^y \bmod n]$, Both the calculations yield $(g^{xy} \bmod n)$.

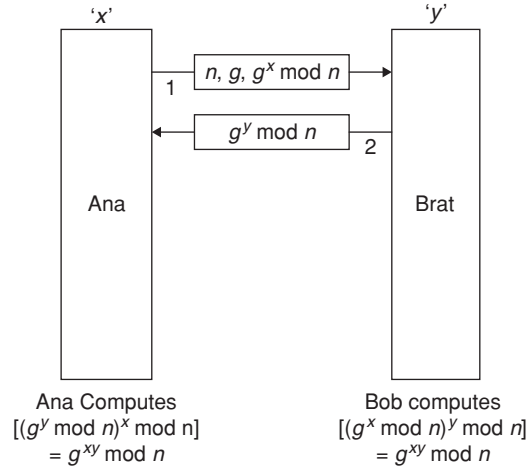


Figure 3 Diffie-Hellman key exchange

RSA (Rivest, Shamir, Adelman)

RSA multiplies large prime numbers together to generate keys. It's strength lies in the fact that it is extremely difficult to factor the product of large prime numbers. This algorithm is the one, most often associated with public key encryption. The RSA algorithm also provides digital signature capabilities.

Example:

- Select two large primes = p, q $p = 17, q = 11$
- $n = p \times q = 17 \times 11 = 187$
- calculate $\phi = (p-1)(q-1) = 16 \times 10 = 160$
- select e, such that LCD $(\phi, e) = 1$, $0 < e < \phi$ say, $e = 7$
- calculate d such that $d \bmod \phi = 1$
- 160k + 1 = 161, 321, 481, 641,
- Check which of these is divisible by 7
- 161 is divisible by 7 giving d = 161/7 = 23
- Key 1 = {7, 187}, key 2 = {23, 187}

Digital Signatures

A digital signature allows a receiver to authenticate (to a limited extent) the identity of the sender and to verify the integrity of the message for the authentication process, you

must already know the senders public key, either from prior knowledge or from some trusted third party. Digital signatures are used to ensure message integrity and authentication. In its simplest from, a digital signature is created by using the senders private key to hash the entire contents of the message being sent to create a message digest. The recipient uses the sender's public key to verity the integrity of the message by recreating the message digest. By this process you ensure the integrity of the message and authenticate the sender.

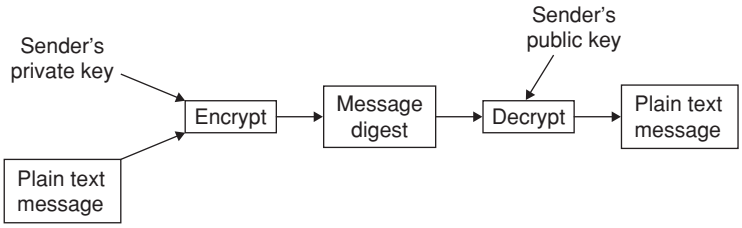


Figure 4 Digital signature

To sign a message, senders usually append their digital signature to the end of a message and encrypt it using the recipient's public key. Recipients decrypt the message using their own private key and verify the sender's identity and the message integrity by decrypting the sender's digital signature using the sender's pubic key. The strength of digital signatures are that they are almost impossible to counterfeit and they are easily verified.

Digital certificate

Digital signatures can be used to verify that a message has been delivered unaltered and to verify the identify of the sender by public key. The problem with authenticating a digital signature, however, is that you must be able to verify that a public key does in fact belong to the individual or entity that claims to have sent it and that the individual or entity is in fact who or what it claims to be.

A digital certificate issued by a certification authority (CA) utilizing a hierarchical public key infrastructure (PKI) can be used to authenticate a sender's identify for spontaneous, first–time contacts. Digital certificates provide a means for secure first time spontaneous communication. A digital certificate provides a high level of confidence in the identify of the individual.

A digital certificate is issued by a trusted/unknown third party (CA) to bind an individual or entity to a public key. The digital certificate is digitally signed by the CA with the CA's private key. This provides independent confirmation that an individual or entity is in fact who it claims to be. The CA issued digital certificates that certify for the identities of those to whom the certificates were issued.

Firewalls

Firewall is a control link between internet and organization intranet. It protects network premises from internet based attacks by providing single choke point. All the network traffic is forced to travel through this fire wall. Firewall allows only authorized traffic to pass through.

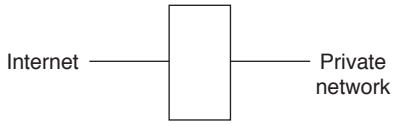
The different types of firewalls are:

1. Packet – filtering router
2. Application level gateways
3. Circuit level gateways
4. Bastion host

Packet filtering router

It filters packets with incoming and outgoing interfaces, and permits or denies certain services. It uses the information of transport layer like IP sources, ICMP message etc.

The drawbacks are IP address spoofing, tiny fragment attack and source routing attacks.



Application level gateway

It provides proxies for each service, when user requests service, it validates the request as legal one and return results to the user.

Application level gateway is more secure than the packet filter.

The drawback of this gateway is processing overhead at each connection.

Circuit-level gateway

It is application level gateway functionality for certain applications. It does not allow end-end TCP connection, rather it maintains two connections, one with the inner host and the other with the outer host. Once the connections are established TCP segment is allowed without examining contents. It only checks the incoming data.

Bastion host

It provides a platform for the application gateway (or) circuit level gateway, it is a critical strong point in network security.

An additional authentication is required for the user who want access to proxy services. Even proxy service authenticates itself before granting the access to user.

Only essential services are installed in the Bastion host which are decided by admin.

EXERCISES

Practice Problems I

Directions for questions 1 to 15: Select the correct alternative from the given choices.

1. In an encryption scheme that uses RSA, values, for p and q are selected to be 5 and 7 respectively what could be the value of d?
(A) 12 (B) 3 (C) 11 (D) 9

2. A person x is supposed to send a document with digitized signature to another person y using public key Cryptography. p is the message. D_x, D_y are private keys of x and y respectively. E_x, E_y are public keys of x, y respectively. Select the best possible sequence of events from below:
(i) $D_x(p)$
(ii) $D_y(p)$
(iii) $E_y(D_x(p))$
(iv) $D_y(D_x(p))$
(v) $D_y(E_y(p))$
(vi) $D_y(E_y(D_x(p))$
(vii) $E_x(D_x(p))$
(viii) $E_y(p)$
(ix) $E_x(D_y(p))$
(x) $D_x(E_y(p))$
(A) (ii), (ix), (viii), (v) (B) (viii), (x), (v), (i)
(C) (i), (iii), (v), (vii) (D) (vii), (v), (iii), (i)

3. Select correct statements about PGP:
(i) Uses existing cryptographic algorithms that have been quite successful.
(ii) Support text compression, digital ignatures.
(iii) Takes plaintext as feed and generates base-64 text.
(iv) No key management capability is rovided.
(A) (i), (ii), (iii) (B) (ii), (iii), (iv)
(C) (i), (iii), (iv) (D) (i), (ii), (iv)

Linked answer questions 4 and 5:

4. Using mono alphabetic substitution a string a b b a c a a b c d is transformed to one of the below strings. Select the most appropriate option:
(A) p q q p r p p s r s (B) j t t x j j i t x t x
(C) u s s u a u u s a b (D) d c c d b b b c b a

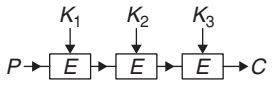
5. Using the mapping obtained above, encrypt the phrase 'bad cab' using same method: Assume space is not encrypted.
(A) q p s r p q (B) t j z x j t
(C) s u b a u s (D) c d a b d c

6. Select the correct statements with regard to packet filters of a firewall:
(i) They are usually driven by a table with information in regards to acceptable sources and destinations.
(ii) Default rules about what needs to be done in regards to packets coming from or going to other machines.
(iii) Can block TCP ports.
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

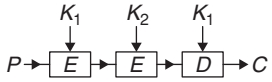
7. What is meant by non-repudiation in the area of digital signatures?
(A) Receiver verifying the signature of the sender.
(B) Receiver concocting the message.
(C) Sender denying having signed digitally.
(D) Receiver changing the contents after receiving the signed document.

8. Which of the following statements about DES is/are true?
(i) DES is public key algorithm.
(ii) DES has 19 distinct stages.
(iii) In the 16 iterations of DES, different keys are used.
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

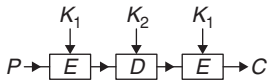
9. Which of the below represents Triple encryption using DES? (P is the unencrypted input, 'C' is encrypted output, k_1, k_2, k_3 are keys used in encryption and decryption, E stands for encryption and D stands for decryption).
(A)



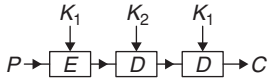
(B)



(C)



(D)



10. Which of the below statements are applied for cipher block chaining?
(i) Each plaintext block is XOR'ed with previous block before encryption.
(ii) Encryption is a mono alphabetic substitution cipher.
(iii) Cipher block chaining can result in same plaintext blocks encrypted to different cipher text blocks.
(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

11. Which of the below statements are applied to RSA algorithm?
(i) RSA is a relatively slow algorithm when encrypting large data.
(ii) Mainly used where key is to be distributed.
(iii) The strength of the algorithm lies in the fact that determining the key can take exceedingly long time by brute force.

(A) (i), (ii) (B) (ii), (iii)
(C) (i), (iii) (D) (i), (ii), (iii)

12. The security and usefulness of a digital signature depends on
(A) A public hash function
(B) A two-way hash function
(C) Protection of user's private key
(D) Protection of user's public key

13. Let '*M*' be the message to be encrypted, *E* be Encryption key and *N* be the product of two random prime numbers, then what is the cipher text using RSA algorithm?
(A) $C = E^m \bmod N$ (B) $C = M^E \bmod N$
(C) $C = N^E \bmod M$ (D) $C = E^N \bmod M$

14. Which of the following best describes the decryption in Triple DES?
(A) Plain text $= D_{K_1}(E_{K_2}(D_{k_1}(\text{ciper text})))$
(B) Plain text $= D_{K_1}(E_{K_2}(D_{k_3}(\text{ciper text})))$
(C) Plain text $= E_{K_1}(D_{K_2}(E_{k_1}(\text{ciper text})))$
(D) Plain text $= E_{K_1}(D_{K_2}(E_{k_1}(\text{ciper text})))$

15. In which cipher mode, all cipher blocks will be chained so that if one is modified the cipher text cannot be decrypted correctly?
(A) Electronic Code Book
(B) Cipher Block Chaining
(C) Cipher Feedback Mode
(D) Counter Mode

Practice Problems 2

Directions for questions 1 to 15: Select the correct alternative from the given choices.

1. 'All algorithms must be public only the keys are secret' is
(A) Rijndael Principle
(B) Kerckhoff's principle
(C) Rivest shamir Adleman principle
(D) None of these

2. Pretty Good Privacy encrypts data by using a block cipher called
(A) RSA (B) MD5
(C) IDEA (D) DES

3. E-mail security package is related to
(A) Pretty Good Privacy
(B) DNS spoofing
(C) Secure Socket Layer
(D) Transport Layer Security

4. Which of the following protocols will be proxy, on an application firewall?
(A) IPX (B) FTP
(C) POP (D) SMS

5. A good recommendation is that if a private key is ____ or longer, the key is thought to be secure.
(A) 40 bits (B) 60 bits
(C) 70 bits (D) 80 bits

6. Which issue is related to server side security?
(A) Protection of the server from legitimate web access
(B) Security of the information stored on server
(C) Security of the customer's physical credit card
(D) Security of the customer's computer

7. Which of the following is not an active attack?
(A) Denial of service (B) Traffic Analysis
(C) Replay (D) Masquerade

8. Verifying the true identity of the sender of a message recipient is known as _____.
(A) Authentication (B) fabrication
(C) Cryptography (D) availability

9. In which of the following techniques, letters are arranged in a different order?
(A) Transposition
(B) Substitution
(C) Private key Encryption
(D) None of the above

10. In which type of attack, Algorithm, cipher text, chosen plaintext and cipher text are known?
(A) Cipher text only
(B) Known plain text
(C) Chosen cipher text
(D) Chosen text

11. In which type of ciphers the encryption depends on current state?
(A) Link cipher
(B) Block cipher
(C) Stream cipher
(D) Current cipher

12. Traffic Analysis can be counted using
(A) Encryption (B) Decryption
(C) Replay (D) Data padding

13. DES Algorithm is vulnerable to
(A) Masquerade attack
(B) Replay attack
(C) Denial of service
(D) Brute Force attack

14. What is the size of key in Triple DES?
(A) 168 bits (B) 112 bits
(C) 56 bits (D) Either (A) or (B) or (C)

15. Direct digital signature involves
(A) Source only
(B) Destination only
(C) Communicating parties, sender and receiver.
(D) Everyone including communicating parties.

Previous Years' Questions

1. Suppose that everyone in a group of N people wants to communicate secretly with the $N-1$ others, using symmetric key cryptographic system. The communication between any two persons should not be decodable by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is **[2015]**

(A) $2N$ (B) $N(N-1)$
(C) $N(N-1)/2$ (D) $(N-1)^2$

2. Consider that B wants to send a message m that is digitally signed to A. Let the pair of private and public keys for A and B be denoted by K_x^- and K_x^+ for $x = A, B$, respectively. Let $K_x(m)$ represent the operation of encrypting m with a key K_x and $H(m)$ represent the message digest. Which one of the following indicates the CORRECT way of sending the message m along with the digital signature to A? **[2016]**

(A) $\{m, K_B^+ (H(m))\}$ (B) $\{m, K_B^- (H(m))\}$
(C) $\{m, K_A^- (H(m))\}$ (D) $\{m, K_A^+ (m)\}$

3. Anarkali digitally signs a message and sends it to Salim. Verification of the signature by Salim requires **[2016]**

(A) Anarkali's public key.
(B) Salim's public key.
(C) Salim's private key.
(D) Anarkali's private key.

4. A sender S sends a message m to receiver R, which is digitally signed by S with its private key. In this scenario, one or more of the following security violations can take place.

(I) S can launch a birthday attack to replace m with a fraudulent message.
(II) A third party attacker can launch a birthday attack to replace m with a fraudulent message.
(III) R can launch a birthday attack to replace m with a fraudulent message.

Which of the following are possible security violations? **[2017]**

(A) (I) and (II) only (B) (I) only
(C) (II) only (D) (II) and (III) only

5. In a RSA cryptosystem, a participant A uses two prime numbers $p = 13$ and $q = 17$ to generate her public and private keys. If the public key of A is 35, then the private key of A is _____. **[2017]**

Answer Keys

Exercises

Practice Problems 1

1. C	**2.** C	**3.** A	**4.** C	**5.** C	**6.** D	**7.** C	**8.** B	**9.** C	**10.** C
11. D	**12.** C	**13.** B	**14.** B	**15.** B					

Practice Problems 2

1. B	**2.** C	**3.** A	**4.** B	**5.** C	**6.** B	**7.** B	**8.** A	**9.** A	**10.** D
11. C	**12.** D	**13.** D	**14.** D	**15.** C					

Previous Years' Questions

1. C	**2.** B	**3.** A	**4.** B	**5.** 11