CRYPTOGRAPHY & NETWORK SECURITY

Attacks on Computers & Computer Security	2
Cryptography: Concepts & Techniques	13
Symmetric Key Algorithm	34
Asymmetric Key Algorithm, Digital Signature and RSA	45
Internet Security Protocols, user Authentication	62
Electronic Mail Security	77
Firewall	82

We ARE MAKAUTIANS

NOTE:

WBUT course structure and syllabus of 8th Semester has been changed from 2014. **CRYPTOGRAPHY & NETWORK SECURITY [CS 801D]** has been introduced in the present curriculum as a new subject. We are providing chapterwise model questions and answers and few relevant WBUT questions & answers along with the complete solutions of new university papers, so that students can get an idea about university questions patterns.

ATTACKS ON COMPUTERS & COMPUTER SECURITY

Multiple Choice Type Questions

1. If the principle of ..... to be ensured the contents of a message must not be modified while in transit. [WBUT 2009]
   a) confidentiality b) authentication c) integrity d) access control

Answer: (c)

2. The .....attack is related to confidentiality [WBUT 2009]
   a) interception b) fabrication c) modification d) interruption

Answer: (a)

3. The principle of ..... ensures that only the sender and the intended recipients have access to the contents of a message. [WBUT 2014]
   a) Confidentiality b) Authentication
   c) Integrity d) Access control

Answer: (a)

4. The .....+..... attack is related to authentication [WBUT 2014]
   a) Interception b) Fabrication c) Modification d) Interruption

Answer: (b)

5. _____ ensures that a message was received by the receiver from the actual sender and not from an attacker. [WBUT 2015]
   a) Authentication b) Authorization
   c) Integration d) None of these

Answer: (a)

6. Which of the following is a passive attack? [WBUT 2015]
   a) Masquerade b) Replay
   c) Denial of service d) Traffic analysis

Answer: (d)

7. A _____ is used to verify the integrity and authenticity of a message [WBUT 2015]
   a) Decryption algorithm b) Message digest
   c) MAC d) both (b) and (c)

Answer: HMAC

8. A macro-virus is [MODEL QUESTION]
   a) platform dependent b) platform independent
   c) idle d) hidden

Answer: (c)

We ARE MAKAUTIANS

9. The four primary security principles related to a message are **[MODEL QUESTION]**

a) confidentiality, authentication, integrity and non-repudiation
b) confidentiality, access control, non-repudiation and integrity
c) authentication, authorization, non-repudiation and availability
d) availability, access control, authorization and authentication

Answer: (a)

10. Which one of the following is active attack? **[MODEL QUESTION]**

a) Masquerade b) Traffic analysis
c) Shoulder surfing d) Evaesdropping

Answer: (a)

11. A virus that cannot be detected by Antivirus Software is **[MODEL QUESTION]**

a) parasitic b) polymorphic c) worm d) stealth

Answer: (d)

12. Interception is an attack on **[MODEL QUESTION]**

a) availability b) confidentiality c) authenticity d) integrity

Answer: (b)

Short Answer Type Questions

1. What is Access Control? How is it different from Availability? **[WBUT 2008]**

Answer:

Access control is a system which enables an authority to control access to areas and resources in a given physical facility or computer-based information system. An access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure.

Access control is broadly related to two areas-

- **Role management:** which concentrate on the user side(which user can do what)
- **Rule management:** which focus on the resources side (which resource is accessible and under what circumstances)

Availability is the assurance that a computer system is accessible by authorized users whenever needed. Two facets of availability are typically discussed:

1. Denial of service.
2. Loss of data processing capabilities as a result of natural disasters (e.g., fires, floods, storms, or earthquakes) or human actions (e.g., bombs or strikes).

However, access control signifies control led access to physically available resources. If availability of resources are blocked by any of the two mechanisms stated above, then we cannot assure any access control.

We ARE MAKAUTIANS

2. Write down the differences between Active attacks and Passive attacks. **[WBUT 2008]**

OR,

Explain active attack and passive attack with example. **[WBUT 2014, 2015]**

Answer:

Active Attacks

In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

Active attacks can be classified into four categories as follows:

- **Masquerade:** In computer terms, 'masquerading' is said to happen when an entity impersonates another. In such an attack, an unauthorized entity tries to gain more privileges than it is authorized for. Masquerading is generally done by using stolen IDs and passwords, or through bypassing authentication mechanisms.
- **Replay:** This active attack involves capturing a copy of the message sent by the original sender and retransmitting it later to bring about an unauthorized result.
- **Modification of messages:** This attack involves making certain modifications to the captured message, or delaying or reodering the messages to cause an unauthorized effect.
- **Denial of service (DoS):** This attack prevents the normal functioning or proper management of communication facilities. For examle, a network server can be overloaded by unwanted packets, thus resulting in performance degradation. DoS attacks can interrupt and slow down the services of a network, or even completely jam a network.

Passive Attacks

A **passive attack** monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. **Passive attacks** include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Two types of passive attacks are:

- **Release of message contents:** This type of passive attack involves (1) capturing the sensitive information that is sent via email or (2) tapping a conversation that is conducted over a telephone line.
- **Traffic analysis:** In this type of attack, an intruder observes the frequency and length of messages being exchanged between communicating nodes. A passive attacker can

We ARE MAKAUTIANS

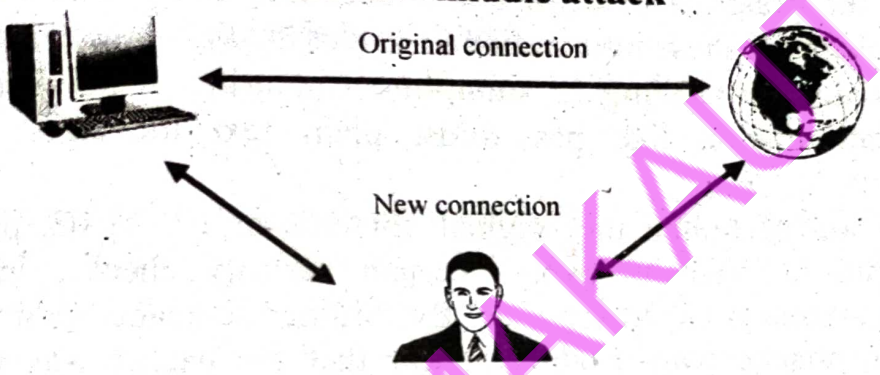
then use this information for guessing the nature of the communication that was taking place.

What is the idea behind man-in-the-middle attack? **[WBUT 2014]**

Answer:

Suppose Alice sends Bob some message, an intruder can act in between Alice and Bob resembling sender and receiver of original message thereby taking control of entire communication that is transmission is either maliciously or fraudulently repeated or delayed. A replay attack occurs when an attacker copies a stream of messages between two parties and replays the stream to one or more of the parties.

Man-in-the-middle attack



4. Distinguish between phishing and pharming. Why is it easy to fall prey to pharming than phishing? **[WBUT 2014]**

Answer:

1st Part:

Both attacks are attempts to get user names and passwords, but they are quite different. Phishing attacks usually will involve an email that appears to be from a company with which we do business prompting us to take action and log in to our account with the link provided in the email. The Web site we visit is not the real site but a cleverly designed imposter site that may seem real to us, so we will enter our username and password, which is then captured by the attacker.

2nd Part:

Pharming is different in that it can happen when we are going to a legitimate Web site, even when we have typed the URL of the Web site ourselves. In a pharming attack, the criminal "hijacks" the intended site's DNS (domain name system) server. The result is that we are redirected an imposter site that looks like our intended site. Many won't notice any difference, will enter their username and password as usual, and the attacker captures it.

WE ARE MAKAUTIANS

5. What are the different types of attacks on computer and network systems? **[WBUT 2014]**

Answer:

- Active attacks alter the system or network operations while passive attack gathers information about the system without altering the system. Active attack can involve infecting the system with virus or worms or can span upto deleting the entire hard drive. Normally passive attacks remain undetected. Active attack can flood the entire network with unnecessary packets and can render it slow while passive attack can sniff network packets without changing them. Different types of active attack includes: masquerade, replay, DOS, DDOS, alteration of message. Passive attackers can know the presence of certain user accounts along with their password while active attackers use these information to render the system useless to the owner.
- **Eavesdropping or sniffing or snooping:** Capturing of network packets to obtain sensitive information like passwords, plain text messages, other confidential information.
- **Spoofing:** Act of hiding the original contents of IP, MAC, protocols with false identification in order to bypass certain security checks, impersonate another computing system is called spoofing. By forging the header so it contains a different address, an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send a response back to the forged source address.
- **Interception:** attacker monitors the stream and gathers information which can be used to organize the attack later on. In this kind of attack the packets intended for the recipient are captured or altered by the attacker in the middle intercepting the packets.
- **Modification Attacks:** the data packets are modified or altered by the attacker if there is no strong encryption method provided and the attacker can intercept and alter the contents violating the integrity of message.
- **Repudiation Attacks:** the sender of the message denies that he is the source of the message. Here the authenticity of the message is violated. Digital signatures are used to prevent these kind of attack.
- **Denial-of-Service (DOS) Attacks and Distributed Denial-of-Service (DDOS) Attacks:** DOS attacks are organized between client and server to flood the network with unnecessary packets. The server is overwhelmed with requests from spoofed addresses and thereby fails to reply services to the original clients. There are different categories of DOS attacks. Some send ICMP echo packets in large quantity while others send SYN packets for TCP connections. Some IP packets are send in large numbers so that original packet size exceeds and server fails to reassemble the packets.
- **Back door Attacks:** attackers plat root kits or Trojans to take control of the system anonymously and without the knowledge of the attacker. They normally open a port or a service which are later exploited.

WeARE MAKAUTians

- **Replay attack or Man-in-the-Middle Attacks:** Alice sends Bob some message, an intruder can act in between Alice and Bob resembling sender and receiver of original message thereby taking control of entire communication that is transmission is either maliciously or fraudulently repeated or delayed. A replay attack occurs when an attacker copies a stream of messages between two parties and replays the stream to one or more of the parties.

Inside attack takes place from inside of secured perimeters of an organization. Normally, Insider has more access to resources of the organization. This may include selling of confidential information of an organization to any competitor. Also time taken by an inside attacker is always less than an outside intruder. Outside attack takes place from remote site or from Internet. Resources gathered by the attacker is less than the previous case. Outside attack may bypass firewall and NAT.

6. What is availability? **[MODEL QUESTION]**

Answer:

By means of the term our goal at Authentify is to provide uninterrupted service 24 hours per day, 7 days a week, 365 days a year. While system maintenance is inevitable, our service level agreements reflect up-time commitments of 99.9% or better.

7. What do you mean by Interruption? **[MODEL QUESTION]**

Answer:

Interruption occurs when resource become unavailable, lost or unusable. Cause of interruption due to failure of computer hardware devices, erasing of program, data or OS

8. What do you mean by computer security and what are its goals? **[MODEL QUESTION]**

Answer:

Computer security is the protection of computing systems and the data that they store or access. Goals of security include

Prevention: Means attack will fail

Detection: Determine an attack (whether underway or already occurred) and report it.

Recovery:

- Stop an attack and assess and repair damage
- Attack is underway but system functions correctly

9. What are the security approaches? **[MODEL QUESTION]**

Answer:

There are two methods to deal with security issues a security policy to define what is, and what is not, allowed and a security mechanism, method / tool / procedure for enforcing a security policy.

WE ARE MAKAUTians

10. What are the basic components of computer security? **[MODEL QUESTION]**

Answer:

Confidentiality: implies to concealment of information or resources. It also applies to the existence of data - sometimes more revealing than data itself.

Integrity: Trustworthiness of data or resource. It generally means - preventing improper or unauthorized change of data. There can be two types of integrity data integrity and origin integrity.

Availability: Availability is the ability to use desired information or resource.

11. What is threat and what are the categories of threat? **[MODEL QUESTION]**

Answer:

Threat is a potential violation of security and a possible danger that might exploit vulnerabilities of a system. There are four broad categories of threat which includes.

Disclosure: It is the act of exposing confidential information. *Snooping* is a form of disclosure

Deception: Act of denying about the source or origin of the message or reception of the same either by sender or receiver. Modification or alteration of message, masquerading or spoofing, repudiation of origin falls under this category.

Disruption: Disruption of service either at the source, in path between source and destination, or at the destination can be achieved by the attackers. Denial of Service (DOS) attack is an example of disruption.

Usurpation: Owning of the host (computer), node (router) or network illegally by the attacker is called usurpation. DDOS is a type of usurpation.

12. What is Brute-force attack? Explain. **[MODEL QUESTION]**

Answer:

In cryptography, a brute-force attack, or exhaustive key search, is a cryptanalytic attack that can, in theory, be used against any encrypted data (except for data encrypted in an information-theoretically secure manner). Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. It consists of systematically checking all possible keys or passwords until the correct one is found. In the worst case, this would involve traversing the entire search space.

When password guessing, this method is very fast when used to check all short passwords, but for longer passwords other methods such as the dictionary attack are used because of the time a brute-force search takes.

When key guessing, the key length used in the cipher determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones. A cipher with a key length of N bits can be broken in a worst-case time proportional to 2N and an average time of half that.

Brute-force attacks can be made less effective by obfuscating the data to be encoded, something that makes it more difficult for an attacker to recognize when he/she has cracked the code. One of the measures of the strength of an encryption system is how

WE ARE MAKAUTIANS

long it would theoretically take an attacker to mount a successful brute-force attack against it.
Brute-force attacks are an application of brute-force search, the general problem-solving technique of enumerating all candidates and checking each one.
The term "brute-force" is not the only term to name such a type of attack. It can also be called "bruteforce", "brute force" and just "brute" (that is common in names of programs that perform brute-force attacks).

Long Answer Type Questions

1. What is the basic difference between worm and virus? **[WBUT 2008]**

Answer:

A computer **virus** attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity: some may cause only mildly annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. Because a virus is spread by human action people will unknowingly continue the spread of a computer virus by sharing infecting files or sending emails with viruses as attachments in the email.

A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line.

Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding. In recent worm attacks such as the much-talked-about Blaster Worm, the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

2. a) What are the key principles of security? **[WBUT 2014]**

OR,

Discuss the basic principle of security. **[WBUT 2015]**

WE ARE MAKAUTIANS

Answer:

Confidentiality: Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. Confidentiality is necessary for maintaining the privacy of the people whose personal information is held in the system.

Integrity: In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner

Availability: For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

Authenticity: In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

Non-repudiation: In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

b) What are meant by IP sniffing and IP spoofing? **[WBUT 2014, 2015]**

Answer:

Sniffing and spoofing are security threats that target the lower layers of the networking infrastructure supporting applications that use the Internet.

Eavesdropping on existing traffic can be called sniffing, for example we can sniff our own traffic using a network sniffer, WireShark is a good tool for this purpose. WireShark does not change the packets and only capture them and display them, this is the meaning of sniffing.

Spoofing is the act of hiding the original contents of IP, MAC, protocols with false identification in order to bypass certain security checks, impersonate another computing system is called spoofing. By forging the header so it contains a different address, an

WE ARE MAKAUTIANS

attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send a response back to the forged source address.

3. Write short notes on the following: **[MODEL QUESTION]**

a) DoS attack

b) Principles of security with example

c) DNS spoofing

Answer:

a) DOS attack:

The denial of service (DoS) has gained a lot of attention in the last few years. The basic purpose of a DoS attack is simply to flood / overhaul a network so as to deny the authentic users services of the network. A DoS attack can be launched in many ways. The end result is the flooding of a network or change in the configuration of routers on the network.

A typical mechanism to launch a DoS attack is with the help of the SYN requests. On the Internet, a client and a server communicate using the TCP/IP protocol. The technique is as follows:-

(i) Client sends a SYN request to the server. A SYN request indicates to the server that the client is requesting for a TCP connection with it.

(ii) The server responds back to the client with an acknowledgement, which is technically called as SYN ACK.

(iii) The client is then expected to acknowledge the server's SYN ACK.

- Packet sniffing is a passive attack on an ongoing conversation. An attacker need not hijack a conservation, but instead, can simply observe (i.e. sniff) packets as they pass by. Clearly, to prevent an attacker from sniffing packets. The entire process is called IP sniffing.
- In this technique, an attacker sends packets with an incorrect source address. When this happens, the receiver would inadvertently send replies back to this forged address (called as spoofed address), and not to the attacker. The entire process is called IP spoofing.

b) Principles of Security:

Let us assume that a person A wants to send a check worth $ 100 to another person B. normally, what are the *a* factors that A and B will think of, in such a case? A will write the check for $ 100, put it inside an envelope, and send it to B.

- A will like to ensure that no one except B gets the envelope, and even if someone else gets it, she does not come to know about the details of the check. This is the principle of **confidentiality.**
- A and B will further like to make sure that no one can tamper with the contents of the check (such as its amount, date, signature, name of the payee, etc.). This is the principle of **integrity.**
- B would like to be assured that the check has indeed come from A, and not from someone else posing as A (as it could be a fake check in that case). This is the principle of **authentication.**

WE ARE MAKAUTIANS

- What will happen tomorrow if B deposits the check in her account, the money is transferred from A's account to B's account, and then A refuses having written/sent the check? The court of law will use A's signature to disallow A to refute this claim, and settle the dispute. This is the principle of **non-repudiation.**

These are the four chief principles of security. There are two more, **access control** and **availability**, which are not related to a particular message, but are linked to the overall system as a whole.

c) DNS spoofing:

DNS spoofing is another one of the man-in-the-middle attacks that can force victims to navigate to a fake website purporting to be a real one.

DNS spoofing is based on presenting fake DNS information to a victim in response to their DNS request and, as a result, forcing them to visit a site which is not the real one.

As an example, suppose the user requests the IP address of mail.yahoo.com, which is supposed to be XX.XX.XX.XX. But the attacker would respond to the DNS query before the actual response arrives with a spoofed address of YY.YY.YY.YY. The user's system will make a connection request to YY.YY.YY.YY, thinking that mail.yahoo.com is located at that IP address. So effectively, the user is routed to a completely different site from the one which he or she originally intended to visit.

Normal DNS communication occurs when the system requests the IP of a particular website and the DNS server responds back with the actual IP address of that website. The system then connects to the website through the IP address it received as a response. With DNS spoofing, the attacker intercepts the DNS request and sends out a response that doesn't contain the actual IP actual, but a spoofed IP address.

To secure yourself from DNS spoofing:

- **Secure your internal systems:** the systems in the internal LAN must be kept secure and updated with the latest security patches from the different vendors. Without this protection, there is a chance one of the systems in the internal LAN will be compromised and start launching DNS spoofing attacks on other LAN systems, further increasing the infections.
- **Deploy IDS/IPS:** intrusion detection systems and intrusion prevention systems are capable of handling DNS spoofing attacks, so they need to be deployed inside the network as well as on the perimeter of the network.
- **DNSSEC:** DNSSEC is a very secure technology that can be used to allow only digitally signed DNS records to be published on DNS servers. Through DNSSEC, we can also prevent bogus zone transfers and hence prevent DNS servers from getting infected themselves.

WE ARE MAKAUTIANS

CRYPTOGRAPHY: CONCEPTS & TECHNIQUES

Multiple Choice Type Questions

1. The matrix theory is used in the ..... technique. [WBUT 2008]
   a) Hill Cipher
   b) Playfair Cipher
   c) Mono-alphabetic Cipher
   d) Vigenere Cipher

Answer: (b)

2. Homophonic Substitution Cipher is ..... to break as compared to Mono-alphabetic Cipher. [WBUT 2008]
   a) easier
   b) the same
   c) difficult
   d) easier or same

Answer: (c)

3. Symmetric key cryptography is .....asymmetric key cryptography. [WBUT 2009]
   a) always slower than
   b) of the same speed as
   c) faster than
   d) usually slower than

Answer: (c)

4. If A and B want to communicate securely with each other, B must not know [WBUT 2009]
   a) A's private key
   b) A's public key
   c) B's private key
   d) B's public key

Answer: (a)

5. Caesar Cipher is an example of [WBUT 2010]
   a) Substitution Cipher
   b) Transposition Cipher
   c) Substitution as well as Transposition Cipher
   d) None of these

Answer: (a)

6. Name the concept that increases the redundancy of plain text. [WBUT 2010]
   a) Confusion
   b) Diffusion
   c) Both (a) and (b)
   d) None of these

Answer: (b)

7. Cryptanalyst is a person who [WBUT 2011]
   a) devises cryptographic solutions
   b) attempts to break cryptographic solutions.
   c) both of these

Answer: (c)

WE ARE MAKAUTIANS

8. The process of writing text as rows and reading it as columns is as [WBUT 2014]
   a) Vernam Cipher
   b) Ceaser Cipher
   c) Columnar Transposition Cipher
   d) Homophonic Substitution Cipher

Answer: (c)

9. In public-key cryptography, _____ key is used for encryption [WBUT 2015]
   a) public
   b) private
   c) both (a) and (b)
   d) shared

Answer: (a)

10. _____ is based on the idea of hiding the relationship between the ciphertext and the key [WBUT 2015]
   a) Diffusion
   b) Confusion
   c) Both (a) and (b)
   d) None of these

Answer: (a)

11. Which of the following is a monoalphabetic cipher? [WBUT 2015]
   a) Caesar cipher
   b) Autokey cipher
   c) Vigenere cipher
   d) All of these

Answer: (a)

12. In polyalphabetic cipher, the characters in plaintext have a _____ relationship with the characters in ciphertext [WBUT 2015]
   a) one-to-one
   b) one-to-many
   c) many-to-one
   d) many-to-many

Answer: (a)

13. Book Cipher is also called as [MODEL QUESTION]
   a) Rail Fence Technique
   b) One-time pad
   c) Mono –alphabetic Cipher
   d) Running Key Cipher

Answer: (d)

14. Conversion of cipher text into plain text is called as [MODEL QUESTION]
   a) encryption
   b) decryption
   c) cryptography
   d) cryptanalyst

Answer: (b)

15. Redundancy of plain text increases by [MODEL QUESTION]
   a) Confusion
   b) Diffusion
   c) Both confusion and diffusion
   d) Neither confusion nor diffusion

Answer: (b)

16. In asymmetric key cryptography keys are required per communicating [MODEL QUESTION]
   a) 2
   b) 3
   c) 4
   d) 5

Answer: (c)

We ARE MAKAUTIANS

Short Answer Type Questions

1. Distinguish between linear and differential cryptanalysis. **[WBUT 2014]**

Answer:

Linear cryptanalysis tries to take advantage of high probability occurrences of **linear** expressions involving plaintext bits, "ciphertext" bits (actually we shall use bits from the 2nd last round output), and subkey bits. It is a known plaintext attack: that is, it is premised on the attacker having information on a set of plaintexts and the corresponding ciphertexts. However, the attacker has no way to select which plaintexts (and corresponding ciphertexts) are available. In many applications and scenarios it is reasonable to assume that the attacker has knowledge of a random set of plaintexts and the corresponding.

Differential cryptanalysis is usually a chosen plaintext attack, meaning that the attacker must be able to obtain encrypted ciphertexts for some set of plaintexts of his choosing. The scheme can successfully cryptanalyze DES with an effort on the order 2^{47} chosen plaintexts. There are, however, extensions that would allow a known plaintext or even a ciphertext-only attack. The basic method uses pairs of plaintext related by a constant *difference*; difference can be defined in several ways, but the exclusive OR (XOR) operation is usual. The attacker then computes the differences of the corresponding ciphertexts, hoping to detect statistical patterns in their distribution. The resulting pair of differences is called a **differential**. Their statistical properties depend upon the nature of the S-boxes used for encryption, so the attacker analyses differentials (Δ_X, Δ_Y), where $\Delta_Y = S(X \text{ (XOR) } \Delta_X) \text{ (XOR) } S(X)$ (for each such S-box S. In the basic attack, one particular ciphertext difference is expected to be especially frequent; in this way, the cipher can be distinguished from random. More sophisticated variations allow the key to be recovered faster than exhaustive search.

2. How does digital envelope exploit the advantages of the both symmetric and asymmetric key cryptography? **[WBUT 2014]**

Answer:

Two primary kinds of encryption are symmetric key and asymmetric key. Symmetric key encryption uses the same key to encrypt and to decrypt. Asymmetric key encryption creates the key in two complementary pieces, like the two pieces of a raggedly torn dollar bill. One piece is the *public key*, because no security is lost by publishing it for anyone to know, and the other is the *private key*, because you must guard it from discovery. If we encrypt with a given public key, someone can decrypt only with the corresponding private key; no other key, *including the public key used to encrypt the information*, can successfully decrypt it. That simple difference in key use is the most significant breakthrough in security technology in 2000 years.

We ARE MAKAUTIANS

3. Is it possible to combine symmetric key and asymmetric key cryptography so that better of the two can be combined? [WBUT 2014]

Answer:

Asymmetric encryption is typically 1000 times slower than symmetric encryption, and the encrypted data it creates is several times larger. One can avoid these limitations by generating a random symmetric key, and using it to encrypt the bulk of the data. The trick is to encrypt the random key using asymmetric encryption with the recipient's public key, and then add it to the encrypted document. The recipient can retrieve the encrypted symmetric key, decrypt it using his or her private key, and then use it to decrypt the remainder of the document. This technique is commonly used; two examples are SSL (which negotiates a symmetric session key for each interaction) and the Windows Encrypting File System (which generates a random symmetric key for each file it encrypts).

4. Explain Vernam cipher. [WBUT 2014, 2015]

Answer:

A Vernam cipher is a symmetrical stream cipher in which the plaintext is XORed with a random or pseudorandom stream of data (the "keystream") of the same length to generate the ciphertext. If the keystream is truly random and used only once, this is effectively a one-time pad. Substituting pseudorandom data generated by a cryptographically secure pseudo-random number generator is a common and effective construction for a stream cipher. RC4 is an example of a Vernam cipher that is widely used on the Internet.

5. What is the difference between block cipher and stream cipher? What are the Different modes of block cipher operation? Explain any one of them. [WBUT 2014]

Answer:

1st Part:

Although both stream ciphers and block ciphers belong to the family of symmetric encryption ciphers, there are some key differences. Block ciphers encrypt fixed length blocks of bits, while stream ciphers combine plain-text bits with a pseudorandom cipher bits stream using XOR operation. Even though block ciphers use the same transformation, stream ciphers use varying transformations based on the state of the engine. Stream ciphers usually execute faster than block ciphers. In terms of hardware complexity, stream ciphers are relatively less complex. Stream ciphers are the typical preference over block ciphers when the plain-text is available in varying quantities (for e.g. a secure wifi connection), because block ciphers cannot operate directly on blocks shorter than the block size. But sometimes, the difference between stream ciphers and block ciphers is not very clear. The reason is that, when using certain modes of operation, a block cipher can be used to act as a stream cipher by allowing it to encrypt the smallest unit of data available.

2nd Part: ***Refer to Question No. 1(a) of Long Answer Type Questions.***

We ARE MAKAUTIANS

6. When an encryption algorithm is said to be computationally secure? **[WBUT 2014]**

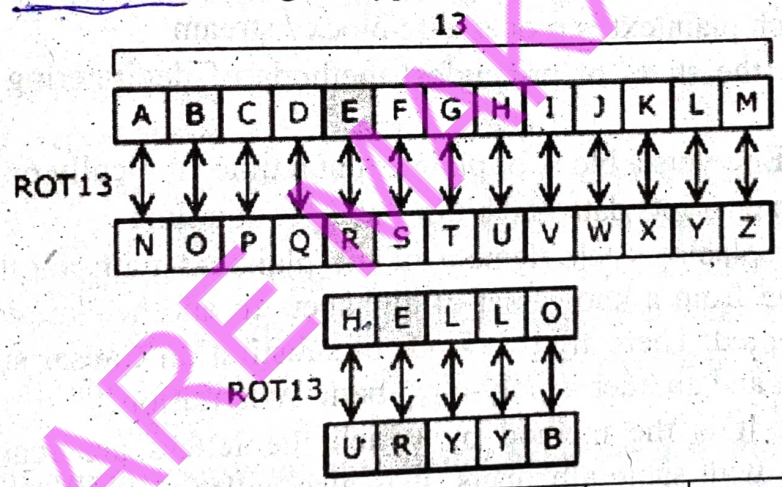
Answer:
The encryption algorithm is said to be computationally secure if
1. The cost of breaking the cipher exceeds the value of the encrypted information
2. The time required to break the cipher exceeds the useful time of the information.

7. Distinguish between substitution and transposition cipher. **[WBUT 2015]**

Answer:
Substitution and transposition ciphers are two categories of ciphers used in classical cryptography. Substitution and transposition differ in how chunks of the message are handled by the encryption process.

Substitution ciphers

Substitution ciphers encrypt plaintext by changing the plaintext one piece at a time. The Caesar Cipher was an early substitution cipher. In the Caesar Cipher, each character is shifted three places up. Therefore, A becomes D and B becomes E, etc…
This table shows "VOYAGER" being encrypted with the Caesar substitution cipher:



Plaintext	V	O	Y	A	G	E	R
Key	+3	+3	+3	+3	+3	+3	+3
Ciphertext	Y	R	B	D	J	H	U

A more complex substitution cipher would be created if, instead of incrementing each character by three, we used a more complex key. This table shows a simple substitution cipher with a key of "123".

Plaintext	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
Key	T	O	E	U	N	Z	I	A	G	X	P	Q	Y	R	H	V	S	M	D	F	C	J	W	B	K	L

Using this substitution cipher to encrypt VOYAGER would give us these results:

Plaintext	V	O	Y	A	G	E	R
Ciphertext	J	H	K	T	X	N	M

The Vernam Cipher, or one time pad, is a simple substitution cipher where the key length equals the message length.
ROT-1 is a simple substitution cipher used to encode messages on Usenet.

WE ARE MAKAUTIANS

Transposition ciphers

Transposition ciphers encrypt plaintext by moving small pieces of the message around. Anagrams are a primitive transposition cipher.

This table shows "VOYAGER" being encrypted with a primitive transposition cipher where every two letters are switched with each other:

V	O	Y	A	G	E	R
O	V	A	Y	E	G	R

8. Define the following terms cryptography, cryptanalysis, block cipher and stream cipher, transposition and substitution, product cipher, public and private key, symmetric and asymmetric cipher. **[MODEL QUESTION]**

Answer:

- **Cryptography:** Cryptography is the study of algorithms to encode plain text. It is characterized by:
  - type of encryption operations used: substitution / transposition / product
  - number of keys used : single-key or secret-key vs. two-key or public-key
  - way in which plaintext is processed : block / stream
- **Cryptanalysis:** the study of principles/ methods of deciphering ciphertext without knowing key
- **Block cipher:** Encrypts a block of plaintext at a time (typically 64 or 128 bits)
- **Stream cipher:** encrypts data one bit or one byte at a time
- **Substitution:** replacing each element of the plaintext with another element. It is a kind of mapping from a known set of alphabets to another known set rendering the plain text encrypted. There are two kinds of substitution Caesar substitution one time pad substitution and another is poly-alphabetic substitution.
- **Transposition:** It is the method by which the letters are rearranged to produce different words with same alphabets. It is also called permutation. Plain text or the key can be used in permutation.
- **Product cipher:** using multiple stages of substitutions and transpositions.
- **Symmetric and asymmetric cipher:** When same key is used to encrypt and decrypt the message it is called symmetric cipher, otherwise it is asymmetric cipher.
- **Public and private key:** In asymmetric cryptography, two different types of keys are used for encryption and decryption. Alice sends a message to Bob over an unsecured system by using Bob's key. This key as known to everybody it is called public key. When Bob receives the message, only he can decrypt it using another key. This key is known to Bob only. This is private key. If anybody else is listening to conversation of Alice and Bob it is made sure that no one else other than Bob can decrypt it.

9. Explain with example the relationship between key size and key range. **[MODEL QUESTION]**

Answer:

The relationship between key size (in bits), time of decryption, number of alternative keys are tabulated below.

WE ARE MAKAUTIANS

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^{6} years

10. What do you mean by encryption and decryption? **[MODEL QUESTION]**

Answer:

The process by which a plain text message is converted to a cipher text is called encryption whereas the reverse process is termed as decryption.

11. What are the different cryptanalysis attack? **[MODEL QUESTION]**

Answer:

Cryptanalysis is the method of obtaining the plain text or the key from encrypted message. There are different types of cryptanalysis attack.

- **ciphertext only:** only know algorithm / ciphertext, statistical, can identify plaintext
- **known plaintext:** know/suspect plaintext & ciphertext to attack cipher
- **chosen plaintext:** select plaintext and obtain ciphertext to attack cipher
- **chosen ciphertext:** select ciphertext and obtain plaintext to attack cipher
- **chosen text:** select either plaintext or ciphertext to en/decrypt to attack cipher

12. What is the difference between unconditionally secure and computationally secure? **[MODEL QUESTION]**

Answer:

A cipher is unconditionally secure if it is secure no matter how much resources (time, space) the attacker has, that is because the amount of data in cipher text is insufficient. All the ciphers we have examined are not unconditionally secure. A cipher is computationally secure if the best algorithm for breaking it will require so much resources (e.g., 1000 years) that practically the cryptosystem is secure.

13. Discuss the relative advantages and disadvantages of a *symmetric key cryptography* vis-à-vis an *Asymmetric key cryptography*. **[MODEL QUESTION]**

Answer:

Refer to Question No. 1(b) of Long Answer Type Questions.

We ARE MAKAUTIANS

14. What are symmetric cipher and asymmetric cipher? **[MODEL QUESTION]**

Answer:

Symmetric cipher:

In a symmetric cipher, both parties must use the same key for encryption and decryption. This means that the encryption key must be shared between the two parties before any messages can be decrypted. Symmetric systems are also known as shared secret systems or private key systems.

Symmetric ciphers are significantly faster than asymmetric ciphers, but the requirements for key exchange make them difficult to use.

Asymmetric cipher:

In an asymmetric cipher, the encryption key and the decryption keys are separate.

In an asymmetric system, each person has two keys. One key, the public key, is shared publicly. The second key, the private key, should never be shared with anyone. When you send a message using asymmetric cryptography, you encrypt the message using the recipients public key.

The recipient then decrypts the message using his private key.

That is why the system is called asymmetric.

15. What are the drawbacks of symmetric cipher? **[MODEL QUESTION]**

Answer:

Drawbacks of symmetric cipher are:

Key distribution

As the keys at both the side should be same, it needs to be exchanged first. So if the media for exchanging the key is compromised, it becomes a disaster.

Compromised KDC

If we are using a key distribution center (KDC) to exchange the keys and the KDC itself is compromised it also becomes a limitation.

Random number generation

We use random numbers for the generation of cipher text in the transformation function. One problem with this random number generator is that the numbers generated will not be perfectly random. So there is a possibility that it can be guessed.

Placement of encryption function

If the encryption function is not properly placed it can lead to leakage of data.

16. What are the problems with exchanging of public keys? **[MODEL QUESTION]**

Answer:

The key exchange problem is how to exchange whatever keys or other information are needed so that no one else can obtain a copy. Historically, this required trusted couriers, diplomatic bags, or some other secure channel. With the advent of public key / private key cipher algorithms, the encrypting key (aka public key) could be made public, since

WE ARE MAKAUTIANS

(at least for high quality algorithms) no one without the decrypting key (aka, the private key) could decrypt the message.

17. "Symmetric key cryptography is faster than Asymmetric key cryptography"- Justify. **[MODEL QUESTION]**

Answer:
Symmetric key encryption is much faster than public key encryption, often by 100 to 1,000 times. Because public key encryption places a much heavier computational load on computer processors than symmetric key encryption, symmetric key technology is generally used to provide secrecy for the bulk encryption and decryption of information.

18. What are the roles of the public and private key? **[MODEL QUESTION]**

Answer:
A user's private key is kept private and known only to the user. The user's public key is made available to others to use. The private key can be used to encrypt a signature that can be verified by anyone with the public key. Or the public key can be used to encrypt information that can only be decrypted by the possessor of the private key

19. a) What are the problems associated with symmetric-key encryption?
b) How those problems can be solved using asymmetric-key encryption? **[MODEL QUESTION]**

Answer:
a) One big issue with using symmetric algorithms is the key exchange problem. The other main issue is the problem of trust between two parties that share a secret symmetric key. Problems of trust may be encountered when encryption is used for authentication and integrity checking.

b) Asymmetric key can be used to verify the identity of the other communicating party. Asymmetric algorithms encrypt and decrypt with different keys. Data is encrypted with a public key, and decrypted with a private key. Generally, symmetric algorithms are much faster to execute on a computer than asymmetric ones. In practice they are often used together, so that a public-key algorithm is used to encrypt a randomly generated encryption key, and the random key is used to encrypt the actual message using a symmetric algorithm. This is sometimes called hybrid encryption.

20. What is key wrapping? How it is useful? **[MODEL QUESTION]**

Answer:
1st Part:
Key Wrap constructions are a class of symmetric encryption algorithms designed to encapsulate (encrypt) cryptographic key material. The Key Wrap algorithms are intended for applications such as (a) protecting keys while in untrusted storage, or (b) transmitting

We ARE MAKAUTIANS

keys over untrusted communications networks. The constructions are typically built from standard primitives such as block ciphers and cryptographic hash functions.
Key Wrap may be considered as a form of key encapsulation algorithm, although it should not be confused with the more commonly known asymmetric (public-key) key encapsulation algorithms (e.g., PSEC-KEM). Key Wrap algorithms can be used in a similar application: to securely transport a session key by encrypting it under a long-term encryption key.

2nd Part:
Key wrapping is used in pure symmetric encryption scenarios. This applies to many applications using password based encryption.
One role of key management is to ensure that the same key used in encrypting a message by a sender is the same key used to decrypt the message by the intended receiver. Thus, if Terry and Pat wish to exchange encrypted messages, each must be equipped to decrypt received messages and to encrypt sent messages. If they use a cipher, they will need appropriate keys. The problem is how to exchange whatever keys or other information are needed so that no one else can obtain a copy.
One solution is to protect the session key with a special purpose long-term use key called a key encrypting key (KEK). KEKs are used as part of key distribution or key exchange. The process of using a KEK to protect session keys is called key wrapping. Key wrapping uses symmetric ciphers to securely encrypt (thus encapsulating) a plaintext key along with any associated integrity information and data. One application for key wrapping is protecting session keys in untrusted storage or when sending over an untrusted transport. Key wrapping or encapsulation using a KEK can be accomplished using either symmetric or asymmetric ciphers. If the cipher is a symmetric KEK, both the sender and the receiver will need a copy of the same key. If using an asymmetric cipher, with public/private key properties, to encapsulate a session key both the sender and the receiver will need the other's public key.

Long Answer Type Questions

1. a) What is Algorithm mode? Describe Cipher Block Chaining (CBC) mode.
[WBUT 2010, 2015]

b) Explain the differences between asymmetric and symmetric key cryptographies.
[WBUT 2010, 2014, 2015]

Answer:
a) 1st Part:
An algorithm mode is a series of a basic algorithm steps of block cipher and some kind of feedback from the precious step.
There are for important algorithm modes,

- Electronic code book (ECB,
- Cipher block chaining (CBC),

WE ARE MAKAUTIANS

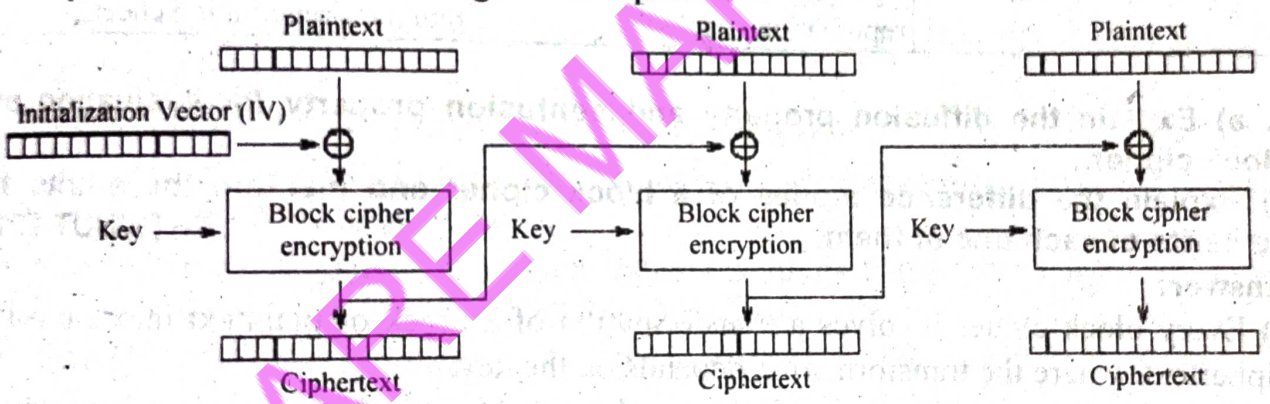
- Cipher feedback (CFB),
- Output feedback (OFB).

2nd Part:

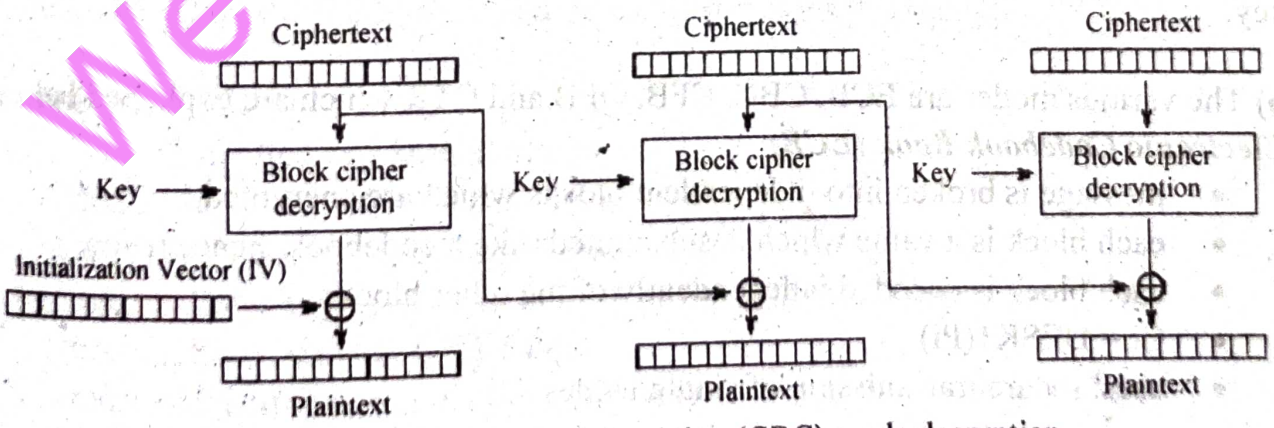
In the **cipher-block chaining** (CBC) mode, each block of plaintext is XORed with the previous cipher text block before being encrypted. This way, each cipher text block is dependent on all plaintext blocks processed up to that point. Also, to make each message unique, an initialization vector must be used in the first block.

CBC has been the most commonly used mode of operation. Its main drawbacks are that encryption is sequential (i.e., it cannot be parallelized), and that the message must be padded to a multiple of the cipher block size. One way to handle this last issue is through the method known as cipher text stealing.

Note that a one-bit change in a plaintext affects all following cipher text blocks. A plaintext can be recovered from just two adjacent blocks of cipher text. As a consequence, decryption *can* be parallelized, and a one-bit change to the cipher text causes complete corruption of the corresponding block of plaintext, and inverts the corresponding bit in the following block of plaintext.



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

We ARE MAKAUTIANS

b) Table: Symmetric versus Asymmetric Key Cryptography

Characteristic	Symmetric key cryptography	Asymmetric key cryptography
1. Key used for encryption/ decryption	Same key is used for encryption and decryption.	One key used for encryption and another, different key is used for decryption.
2. Speed of encryption/ decryption.	Very fast.	Slower.
3. Size of resulting encrypted text	Usually same as or less than the original clear text size.	More than the original clear text size.
4. Key agreement /exchange	A big problem.	No problem at all.
5. Number of keys required as compared to the number of participants in the message exchange.	Equals about the square of the number of participants, so scalability is an issue.	Same as the number of participants, so scales up quit well.
6. Usage.	Mainly for encryption and decryption (confidentiality), signatures (integrity and non-repudiation checks).	Can be used for encryption and decryption (confidentiality) as well as for digital signatures (integrity and non-repudiation checks).

2. a) Explain the diffusion property and confusion property for evaluation of a block cipher.

b) Explain the difference modes of a block cipher and mention the merits and demerits of each one of them. **[WBUT 2011]**

Answer:

a) Every block cipher involves a transformation of a block of plaintext into a block of ciphertext, where the transformation depends on the key.

The mechanism of diffusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key.

b) The various modes are ECB, CBC, CFB, OFB and CTR which are explained below:

Electronic Codebook Book (ECB)

- message is broken into independent blocks which are encrypted.
- each block is a value which is substituted, like a codebook, hence name.
- each block is encoded independently of the other blocks
- Ci = DESK1(Pi)
- uses secure transmission of single values

Advantages and Limitations of ECB

- repetitions in message may show in ciphertext
- if aligned with message block
- particularly with data such graphics

WE ARE MAKAUTIANS

- or with messages that change very little, which become a code-book analysis problem
- weakness due to encrypted message blocks being independent
- main use is sending a few blocks of data.

Cipher Block Chaining (CBC)

- message is broken into blocks
- but these are linked together in the encryption operation
- each previous cipher blocks is chained with current plaintext block, hence name
- use Initial Vector (IV) to start process
- Ci = DESK1(Pi XOR Ci-1)
- C-1 = IV
- uses: bulk data encryption, authentication

Advantages and Limitations of CBC

- each ciphertext block depends on all message blocks
- thus a change in the message affects all ciphertext blocks after the change as well as the original block
- need Initial Value (IV) known to sender & receiver
- however if IV is sent in the clear, an attacker can change bits of the first block, and change IV to compensate
- hence either IV must be a fixed value (as in EFTPOS) or it must be sent encrypted in ECB mode before rest of message
- at end of message, handle possible last short block
- by padding either with known non-data value (e.g. nulls)
- or pad last block with count of pad size
- e.g. [b1 b2 b3 0 0 0 0 5] <- 3 data bytes, then 5 bytes pad+count.

Cipher FeedBack (CFB)

- message is treated as a stream of bits
- added to the output of the block cipher
- result is feedback for next stage (hence name)
- standard allows any number of bit (1,8 or 64 or whatever) to be feed back
- denoted CFB-1, CFB-8, CFB-64 etc
- is most efficient to use all 64 bits (CFB-64)
- Ci = Pi XOR DESK1(Ci-1)
- C-1 = IV
- uses: stream data encryption, authentication.

WE ARE MAKAUTIANS

Advantages and Limitations of CFB

- appropriate when data arrives in bits/bytes
- most common stream mode
- limitation is need to stall while do block encryption after every n-bits
- note that the block cipher is used in encryption mode at both ends
- errors propagate for several blocks after the error.

Output FeedBack (OFB)

- message is treated as a stream of bits
- output of cipher is added to message
- output is then feedback (hence name)
- feedback is independent of message
- can be computed in advance
- Ci = Pi XOR Oi
- Oi = DESK1(Oi-1)
- O-1 = IV
- uses: stream encryption over noisy channels.

Advantages and Limitations of OFB

- used when error feedback a problem or where need to encryptions before message is available
- superficially similar to CFB
- but feedback is from the output of cipher and is independent of message
- a variation of a Vernam cipher
- hence must never reuse the same sequence (key+IV)
- sender and receiver must remain in sync, and some recovery method is needed to ensure this occurs
- originally specified with m-bit feedback in the standards
- subsequent research has shown that only **OFB-64** should ever be used

Counter (CTR)

- similar to OFB but encrypts counter value rather than any feedback value
- must have a different key & counter value for every plaintext block (never reused)
- Ci = Pi XOR Oi
- Oi = DESK1(i)
- uses: high-speed network encryptions.

We ARE MAKAUTIANS

Advantages and Limitations of CTR

- efficiency
- can do parallel encryptions
- in advance of need
- good for bursty high speed links
- random access to encrypted data blocks
- provable security (good as other modes)
- but must ensure never reuse key/counter values, otherwise could break

3. a) What would be the transformation of a message "Happy birthday to you" using Rail Fence technique? **[WBUT 2014]**

Answer:

H				y				t				y				o	
	a		p		b		r		h		a		t		y		u
		p				i				d				o			

So the transformed message is - Hyt yoa pbr hat yup ido

b) For a Vernam Cipher do the following: **[WBUT 2014]**

i) Using pad "TZQ" encode "ARE"

ii) Using pad "ARX" decode "YFR"

Answer:

Consider the following table:

Letter	Bit sequence	Letter	Bit sequence
A	00000	Q	10000
B	00001	R	10001
C	00010	S	10010
D	00011	T	10011
E	00100	U	10100
F	00101	V	10101
G	00110	W	10110
H	00111	X	10111
I	01000	Y	11000
J	01001	Z	11001
K	01010	0	11010
I	01011	1	11011
M	01100	2	11100
N	01101	3	11101
O	01110	4	11110
P	01111	-	11111

We ARE MAKAUTIANS

i)

A- 00000	R-10001	E- 00100
T- 10011	Z- 11001	Q- 10000

XOR

T- 10011	I- 01000	U- 10100

So the cipher text will be TIU

ii)

Y- 11000	F- 00101	R- 10001
A- 00000	R- 10001	X- 10111

XOR

Y- 11000	U- 10100	G- 00110

So the plain text will be YUG

4. Write short note on public key infrastructure. **[WBUT 2015]**

Answer:

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party.

Without PKI, sensitive information can still be encrypted (ensuring confidentiality) and exchanged, but there would be no assurance of the identity (authentication) of the other party. Any form of sensitive data exchanged over the Internet is reliant on PKI for security.

Elements of PKI

A typical PKI consists of hardware, software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates. Digital certificates are at the heart of PKI as they affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate.

A typical PKI includes the following key elements:

- A trusted party, called a **certificate authority (CA),** acts as the root of trust and provides services that authenticate the identity of individuals, computers and other entities
- A **registration authority**, often called a subordinate CA, certified by a root CA to issue certificates for specific uses permitted by the root
- **A certificate database**, which stores certificate requests and issues and revokes certificates

We ARE MAKAUTIANS

- A **certificate store**, which resides on a local computer as a place to store issued certificates and private keys

A CA issues digital certificates to entities and individuals after verifying their identity. It signs these certificates using its private key; its public key is made available to all interested parties in a self-signed CA certificate. CAs uses this trusted root certificate to create a "chain of trust" -- many root certificates are embedded in Web browsers so they have built-in trust of those CAs. Web servers, email clients, smartphones and many other types of hardware and software also support PKI and contain trusted root certificates from the major CAs.

Along with an entity's or individual's public key, digital certificates contain information about the algorithm used to create the signature, the person or entity identified, the digital signature of the CA that verified the subject data and issued the certificate, the purpose of the public key encryption, signature and certificate signing, as well as a date range during which the certificate can be considered valid.

5. a) What is the principle behind One-Time Pads? Why are they highly secured?
b) What is the output of the following Plaintext:
"I am a student of fourth year Information Technology department."
[MODEL QUESTION]

Answer:

a) In cryptography, a one-time pad is a system in which a private key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages. Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected. With a one-time pad, however, the decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely or how to keep both keys secure. One-time pads have sometimes been used when the both parties started out at the same physical location and then separated, each with knowledge of the keys in the one-time pad. The key used in a one-time pad is called a secret key because if it is revealed, the messages encrypted with it can easily be deciphered. One-time pads figured prominently in secret message transmission and espionage before and during World War II and in the Cold War era. On the Internet, the difficulty of securely controlling secret keys led to the invention of public key cryptography.

b) If we use a route cipher of dimension 6 × 9 then we get the table as below:

I	A	M	A	S	T	U	D	E
N	T	O	F	F	O	U	R	T
H	Y	E	A	R	I	N	F	O
R	M	A	T	I	O	N	T	E
C	H	N	O	L	O	G	Y	D
E	P	A	R	T	M	E	N	T

WeARE MAKAUTIANS

So the cipher text will be
ETOEDTNEMTRAPECRHNIAMASTUDRFTYGOLONHMYTOFFOUNNOITAEARI

6. Briefly describe the Knapsack algorithm for public key encryption.
[MODEL QUESTION]

Answer:

Creating the public/private key

First we have to choose a super-increasing knapsack (to use as the private key) with which to encrypt our data. To keep it simple, in my knapsack, we have objects of the following weights: {1, 7, 9, 18, 50, 86}

Now we pick a modulus, m, which is bigger than the sum of all the elements. With my knapsack, the total weight is 171, so 175 would be a suitable value, so m=175.

We then pick a number, n, that is less than, and relatively prime to (that is, sharing no factors beside 1 with) m. We will take n=27.

We then multiply each element in my knapsack by n mod m. This gives me:

1* 27 mod 175 = 27
7 * 27 mod 175 = 14
9 * 27 mod 175 = 68
18 * 27 mod 175 = 136
50 * 27 mod 175 = 125
86 * 27 mod 175 = 47

This creates the knapsack {27, 14, 68, 136, 125, 47}. This will be our public key because, as the subset-sum problem demonstrates, solving this will be ***hard*** because it is not super-increasing.

Encryption

Now we need something to encrypt. For example 01010101 11001100 00100101

First we break it up into blocks that are the length of our knapsack, so: 010101 011100 110000 100101

If we look at the first block (010101), there are 1's in the second, fourth and sixth positions. This means that we take the second, fourth and sixth numbers in our public key, and add them together:

14+136+47 = 197

Repeating this for the other 3 blocks gives us:

011100 = 14 + 68 + 136 = 218
110000 = 27 + 14 = 41
100101 = 27 + 136 + 47 = 210

This gives us the encrypted version of 01010101 11001100 00100101 as {197, 218, 41, 210}. This encrypted data would then be transmitted to the recipient.

We ARE MAKAUTIANS

We know that the subset-sum problem is ***easy*** to solve using a super-increasing set and since our private key is super-increasing we can send them this along with m and n (as chosen earlier), to enable them to decrypt the message.

Decryption

Decrypting the message is the same as solving the subset-sum problem with the original, decrypted message as our target. First we need to solve:

$(x * 27) \bmod 175 = 1$ so that we can move from the **hard** non-super-increasing set to the **easy** super-increasing set.

In this case, $x = 13$.

We can then do

$(13 * 197) \bmod 175 = 111$ to translate the target of the hard to solve problem to the target of the easy to solve problem. If we look at the private key ({1, 7, 9, 18, 50, 86 }), we can easily see that 111 is made up of 86 + 18 + 7. Since these correspond to the second, fourth and sixth values in the key, we can convert this to 010101. Repeating this with the other parts of the encrypted data will reveal the whole message.

7. Write short notes on the following: **[MODEL QUESTION]**

i) Caesar cipher

ii) Vigenère cipher

iii) Playfair or earlier block cipher

iv) Steganography

Answer:

i) Caesar cipher:

Earliest known substitution cipher. Invented by Julius Caesar. In this type of encryption each letter is replaced by the letter three positions further down the alphabet.

- Plain: 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
- Cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
- Example: ohio state à RKLR VWDWH
- Mathematically, map letters to numbers:

a, b, c, ..., x, y, z

0, 1, 2, ..., 23, 24, 25

1. Then the general Caesar cipher is:

$c = E_K(p) = (p + k) \bmod 26$

$p = D_K(c) = (c - k) \bmod 26$

- Can be generalized with any alphabet.

ii) Vigenère cipher:

An early stream cipher is commonly ascribed to the Frenchman Blaise de Vigenère, a diplomat who served King Charles IX. It works by adding a key repeatedly into the plaintext using the convention that A = 0, B = 1, . . . , Z = 25; and addition is carried out modulo 26—that is, if the result is greater than 25, we subtract as many multiples of 26 as

WE ARE MAKAUTIANS

are needed to bring us into the range [0, . . . ,25], that is, [A, . . . ,Z]. Mathematicians write this as: $C = P + K \bmod 26$

For example, when we add P(15) to U(20) we get 35, which we reduce to 9 by subtracting 26; 9 corresponds to J, so the encryption of P under the key U (and of U under the key P) is J. Vigenère used a repeating key, also known as a *running key*. Various means were developed to do this addition quickly, including printed tables and, for field use, cipher wheels.

iii) Playfair or earlier block cipher:

One of the best-known early block ciphers is the Playfair system. It was invented in 1854 by Sir Charles Wheatstone, a telegraph pioneer who also invented the concertina and the Wheatstone bridge. This cipher uses a 5 by 5 grid, in which the alphabet is placed, permuted by the keyword, and omitting the letter J . The plaintext is first conditioned by replacing J with I wherever it occurs, then dividing it into letter pairs, preventing double letters occurring in a pair by separating them with an x, and finally adding a z if necessary to complete the last letter pair. The example Playfair written was "Lord Granville's letter," which becomes "lo rd gr an vi lx le sl et te rz". It is then enciphered two letters at a time using the following rules:

- If two letters are in the same row or column, they are replaced by the succeeding letters. For example, "am" enciphers to "LE."
- Otherwise, the two letters stand at two of the corners of a rectangle in the table, and we replace them with the letters at the other two corners of this rectangle.

Steps:

- Use a 5 x 5 matrix.
- Fill in letters of the key (w/o duplicates).
- Fill the rest of matrix with other letters.
- E.g., key = MONARCHY.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Playfair ciphertexts do look random, but they have the property that if you change a single letter of a plaintext pair, then often only a single letter of the ciphertext will change.

iv) Steganography:

It is the process of hiding a message in another message.

- E.g., hide your plaintext in a graphic image
- Each pixel has 3 bytes specifying the RGB color

WeARE MAKAUTIANS

- The least significant bits of pixels can be changed w/o greatly affecting the image quality
- So can hide messages in these LSBs. Take a 640x480 (=30,7200) pixel image.
- Using only 1 LSB, can hide 115,200 characters
- Advantage: hiding existence of messages
- Drawback: high overhead.

We ARE MAKAUTIANS

SYMMETRIC KEY ALGORITHM

Multiple Choice Type Questions

1. In IDEA, the key size is ..... bits. [WBUT 2014]
   a) 128 b) 64 c) 256 d) 512
   Answer: (a)

2. There are _____ encryption rounds in IDEA. [WBUT 2015]
   a) 5 b) 16 c) 10 d) 8
   Answer: (d)

3. Bits contain in DES encrypts blocks. [MODEL QUESTION]
   a) 32 b) 56 c) 64 d) 128
   Answer: (c)

4. DES encrypts blocks of _____ bits. [MODEL QUESTION]
   a) 32 b) 56 c) 64 d) 128
   Answer: (c)

5. In DES encryption algorithm, which of the following is used for converting 32-bit right half into 48-bits? [MODEL QUESTION]
   a) Permutation b) Expansion permutation
   c) Substitution d) Key scheduling
   Answer: (a)

Short Answer Type Questions

1. What is initializing Vector (IV)? What is its significance? [WBUT 2014]

Answer:

An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session.

The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher. For example, a sequence might appear twice or more within the body of a message. If there are repeated sequences in encrypted data, an attacker could assume that the corresponding sequences in the message were also identical. The IV prevents the appearance of corresponding duplicate character sequences in the cipher text.

The ideal IV is a random number that is made known to the destination computer to facilitate decryption of the data when it is received. The IV can be agreed on in advance, transmitted independently or included as part of the session setup prior to exchange of the message data. The length of the IV (the number of bits or bytes it contains) depends on

WE ARE MAKAUTIANS

the method of encryption. The IV length is usually comparable to the length of the encryption key or block of the cipher in use.

2. Describe briefly DES algorithm.

[WBUT 2014, 2015-Short Note]

Answer:

The modified Lucifer algorithm was adopted by NIST as a federal standard on November 23, 1976. Its name was changed to the Data Encryption Standard (DES).It takes a 64-bit block of plaintext as input and outputs a 64-bit block of ciphertext. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm, DES is both a block cipher and a product cipher. DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the ciphertext. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially. To do the encryption, DES uses "keys" where are 64 bits long. However, every 8th key bit is ignored in the DES algorithm, so that the effective key size is 56 bits. But, in any case, 64 bits (16 hexadecimal digits) is the round number upon which DES is organized.

For example, if we take the plaintext message "8787878787878787", and encrypt it with the DES key "0E329232EA6D0D73", we end up with the ciphertext "0000000000000000". If the ciphertext is decrypted with the same secret DES key "0E329232EA6D0D73", the result is the original plaintext "8787878787878787".

3. Explain Simple Columnar Transposition Technique of symmetric encryption. Convert the text "WEST BENGAL UNIVERSITY OF TECHNOLOGY" with the key value 31254.

[MODEL QUESTION]

Answer:

1st Part:

The Simple Columnar Transposition Technique is the variation of the Rail Fence Technique. This technique simply arrange the plain text as a sequence of rows of the rectangle that are read in column randomly. The Simple Columnar Transposition Technique is also used multiple rounds to provide a tight security. Ciphertext produced by using Simple Columnar Transposition Technique with multiple rounds is much more complex to crack as compare to the basic technique.

2nd Part:

SGIITOWEUROHGENNSFNYBLEYCOTAVTEL

4. What is the purpose of the S-boxes in DES?

[MODEL QUESTION]

Answer:

The S-boxes are the nonlinear part of DES that makes it difficult to break the algorithm and secure against linear and differential cryptanalysis. the s-boxes provide the "confusion" of data and key values, whilst the permutation P then spreads this as widely as possible, so each S-box output affects as many S-box inputs in the next round as possible, giving "diffusion".

WE ARE MAKAUTIANS

There are 8 s-boxes also known as the substitution boxes, is a table that consist of four rows and 16 columns with 64 entries all together. They take in 6-bits and produce or output 4-bits. That is, the 48-bits into 8 S-boxes will be 6-bits each. However the 6-bits is represented in binary form of say, 010100. The two outer bits (the first and the last bit) represents the row (one of the four rows) and the inner four bits represent the columns (one of the 16 columns). The cell where the row and the column meets represents the value in decimal of the output. This is then converted to binary as the output. From the example 010100. the first and last digits 00 = the row which is the first row (00, 01, 10, 11) and the inner four digits 1010= the column. All 8 S-boxes will output 4-bits each in similar way and that is 32-bits output that is then permutated and further processed in the next round.

5. a) What is a meet-in-the-middle attack? **[MODEL QUESTION]**
b) Why is the middle portion of 3DES a decryption rather than an encryption?

Answer:

a) It's that attack doesn't depend on any particular property of the DES, instead, it will work against any type of block ciphers.

For the double-DES cipher & a given (P,C) pair, this attack works as follow:

1. Encrypt the plaintext P with all possibilities of K1, store the results in a table, & sort that table by the value of X.
2. Decrypt C with all possible values of K2, check each resulted value with the entries in the table, in case of match, check these two keys against another known pair (P1,C1), if match, accept them as the correct keys.

b)

1. It's a decryption process in order to change the traditional nature of the DES, if it's an encryption, it'll stay a DES but with longer key size.
2. In the cryptography, there is no significance of using the decryption in the middle stage, the only advantage of doing so is to allow users of 3DES to decrypt data encrypted by the users of the older single DES

   ➔ C = Ek1[Dk2[Ek1[P]]] = Ek1[P].

   Suppose that the middle portion is decryption instead of encryption,

   ➔ C = Ek1[Ek2[Ek1[P]]]

   The previous assumption in equation 1 will not be ever met. On the other hand
3. If an encryption process is done instead of decryption the meet-in-the-middle attack becomes possible.

6. What is symmetric key cryptography? **[MODEL QUESTION]**

Answer:

Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. Symmetric key cryptography consists of the following terms:

WE ARE MAKAUTIANS

1. **Plaintext:** This is the original intelligible message or data that is fed to the algorithm as input.
2. **Encryption algorithm:** The encryption algorithm performs various substitutions and permutations on the plaintext
3. **Secret Key:** The secret key is also input to the encryption algorithm. The exact substitutions and permutations performed depend on the key used, and the algorithm will produce a different output depending on the specific key being used at the time.
4. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the key. The ciphertext is an apparently random stream of data, as it stands, is unintelligible.
5. **Decryption Algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

7. What do you mean by the cryptographic terms confusion and diffusion? [MODEL QUESTION]

Answer:

By confusion we mean that a cipher should hide local patterns in language from an attacker. By diffusion we mean that the cipher should mix around different parts of the plaintext, so that nothing is left in its original position. A polyalphabetic substitution cipher such as the Vignere cipher is more effective at confusion. Symmetric cipher is the Data Encryption Standard (DES) is an example of both confusion and diffusion.

8. What are the different types of symmetric key encryption? [MODEL QUESTION]

Answer:

Types of symmetric key ciphers are

- Block Ciphers: Symmetric key ciphers, where a block of data is encrypted
- Stream Ciphers: Symmetric key ciphers, where block size=1

9. What are the modes of operation of Block cipher? [MODEL QUESTION]

Answer:

Block ciphers can operate in several modes like Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) mode and Output Feedback (OFB) etc.

10. What is the key size of IDEA? [MODEL QUESTION]

Answer:

IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key and there are 8 rounds of transformation.

11. How the keys are generated in IDEA? [MODEL QUESTION]

Answer:

128 bit key is transformed into 16 bit subkey for 8 rounds. 64-bit plaintext block is partitioned into four 16-bit sub-blocks. Then keys are operated on 16 bit sub-blocks in 8 rounds subsequently. The 52 16-bit key sub-blocks which are generated from the 128-bit key are produced as follows:

WE ARE MAKAUTIANS

- First, the 128-bit key is partitioned into eight 16-bit sub-blocks which are then directly used as the first eight key sub-blocks.
- The 128-bit key is then cyclically shifted to the left by 25 positions, after which the resulting 128-bit block is again partitioned into eight 16-bit sub-blocks to be directly used as the next eight key sub-blocks.
- The cyclic shift procedure described above is repeated until all of the required 52 16-bit key sub-blocks have been generated.

12. What are the drawbacks of DES? **[MODEL QUESTION]**

Answer:

The Data Encryption Standard (DES) algorithm has been a popular secret key encryption algorithm and is used in many commercial and financial applications. Although introduced in 1976, it has proved resistant to all forms of cryptanalysis. However, its key size is too small by current standards and its entire 56 bit key space can be searched in approximately 22 hours.

13. What do you understand by the term modes of operation? **[MODEL QUESTION]**

Answer:

Electronic Code Book (ECB) mode: A block cipher encrypts and decrypts plaintext in fixed-size-bit blocks (mostly 64 and 128 bit). For plaintext exceeding this fixed size, the simplest approach is to partition the plaintext into blocks of equal length and encrypt each separately. This method is named Electronic Code Book (ECB) mode. However, Electronic Code Book is not a good system to use with small block sizes (for example, smaller than 40 bits) and identical encryption modes. As ECB has disadvantages in most applications, other methods named modes have been created.

In cipher block chaining, or CBC, mode we exclusive-or the previous block of cipher text to the current block of plaintext before encryption. This mode is effective at disguising any patterns in the plaintext: the encryption of each block depends on all the previous blocks. The input IV is an initialization vector, a random number that performs the same function as a seed in a stream cipher, and ensures that stereotyped plaintext message headers won't leak information by encrypting to identical cipher text blocks. Others modes include, Cipher Feedback (CFB) and Output Feedback (OFB) modes.

14. What are the advantages of IDEA? **[MODEL QUESTION]**

Answer:

The IDEA encryption algorithm

- provides high level security not based on keeping the algorithm a secret, but rather upon ignorance of the secret key
- is fully specified and easily understood
- is available to everybody
- is suitable for use in a wide range of applications
- can be economically implemented in electronic components (VLSI Chip)
- can be used efficiently

WE ARE MAKAUTIANS

- may be exported world wide
- is patent protected to prevent fraud and piracy

15. What are the applications of IDEA? **[MODEL QUESTION]**

Answer:

Today, there are hundreds of IDEA-based security solutions available in many market areas, ranging from Financial Services, and Broadcasting to Government. IDEA is the name of a proven, secure, and universally applicable block encryption algorithm, which permits effective protection of transmitted and stored data against unauthorized access by third parties. The fundamental criteria for the development of IDEA were highest security requirements along with easy hardware and software implementation for fast execution. The IDEA algorithm can easily be embedded in any encryption software. Data encryption can be used to protect data transmission and storage. Typical fields are:

- Audio and video data for cable TV, pay TV, video conferencing, distance learning, business TV, VoIP
- Sensitive financial and commercial data
- Email via public networks
- Transmission links via modem, router or ATM link, GSM technology
- Smart cards

Long Answer Type Questions

1. State and explain how IDEA works. **[WBUT 2015]**

Answer:

IDEA was to develop a strong encryption algorithm, which would replace the DES procedure developed in the U.S.A. in the seventies. It is also interesting in that it entirely avoids the use of any lookup tables or S-boxes. When the famous PGP email and file encryption product was designed by Phil Zimmermann, the developers were looking for maximum security. IDEA was their first choice for data encryption based on its proven design and its great reputation.

The IDEA encryption algorithm

- provides high level security not based on keeping the algorithm a secret, but rather upon ignorance of the secret key
- is fully specified and easily understood
- is available to everybody
- is suitable for use in a wide range of applications
- can be economically implemented in electronic components (VLSI Chip)
- can be used efficiently
- may be exported world wide
- is patent protected to prevent fraud and piracy

WeARE MAKAUTIANS

Description of IDEA

The block cipher IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key. The fundamental innovation in the design of this algorithm is the use of operations from three different algebraic groups. The substitution boxes and the associated table lookups used in the block ciphers available to-date have been completely avoided. The algorithm structure has been chosen such that, with the exception that different key sub-blocks are used, the encryption process is identical to the decryption process.

Key Generation

The 64-bit plaintext block is partitioned into four 16-bit sub-blocks, since all the algebraic operations used in the encryption process operate on 16-bit numbers. Another process produces for each of the encryption rounds, six 16-bit key sub-blocks from the 128-bit key. Since a further four 16-bit key-sub-blocks are required for the subsequent output transformation, a total of 52 (= 8 × 6 + 4) different 16-bit sub-blocks have to be generated from the 128-bit key.

The key sub-blocks used for the encryption and the decryption in the individual rounds are shown in Table 1.

Encryption of the key sub-blocks

Round 1	$Z_1^{(1)}Z_2^{(1)}Z_3^{(1)}Z_4^{(1)}Z_5^{(1)}Z_6^{(1)}$
Round 2	$Z_1^{(2)}Z_2^{(2)}Z_3^{(2)}Z_4^{(2)}Z_5^{(2)}Z_6^{(2)}$
Round 3	$Z_1^{(3)}Z_2^{(3)}Z_3^{(3)}Z_4^{(3)}Z_5^{(3)}Z_6^{(3)}$
Round 4	$Z_1^{(4)}Z_2^{(4)}Z_3^{(4)}Z_4^{(4)}Z_5^{(4)}Z_6^{(4)}$
Round 5	$Z_1^{(5)}Z_2^{(5)}Z_3^{(5)}Z_4^{(5)}Z_5^{(5)}Z_6^{(5)}$
Round 6	$Z_1^{(6)}Z_2^{(6)}Z_3^{(6)}Z_4^{(6)}Z_5^{(6)}Z_6^{(6)}$
Round 7	$Z_1^{(7)}Z_2^{(7)}Z_3^{(7)}Z_4^{(7)}Z_5^{(7)}Z_6^{(7)}$
Round 8	$Z_1^{(8)}Z_2^{(8)}Z_3^{(8)}Z_4^{(8)}Z_5^{(8)}Z_6^{(8)}$
Output Transform	$Z_1^{(9)}Z_2^{(9)}Z_3^{(9)}Z_4^{(9)}$

The 52 16-bit key sub-blocks which are generated from the 128-bit key are produced as follows:

- First, the 128-bit key is partitioned into eight 16-bit sub-blocks which are then directly used as the first eight key sub-blocks.
- The 128-bit key is then cyclically shifted to the left by 25 positions, after which the resulting 128-bit block is again partitioned into eight 16-bit sub-blocks to be directly used as the next eight key sub-blocks.
- The cyclic shift procedure described above is repeated until all of the required 52 16-bit key sub-blocks have been generated.

We ARE MAKAUTIANS

Encryption

The functional representation of the encryption process is shown in Figure 1. The process consists of eight identical encryption steps (known as encryption rounds) followed by an output transformation. The structure of the first round is shown in detail.

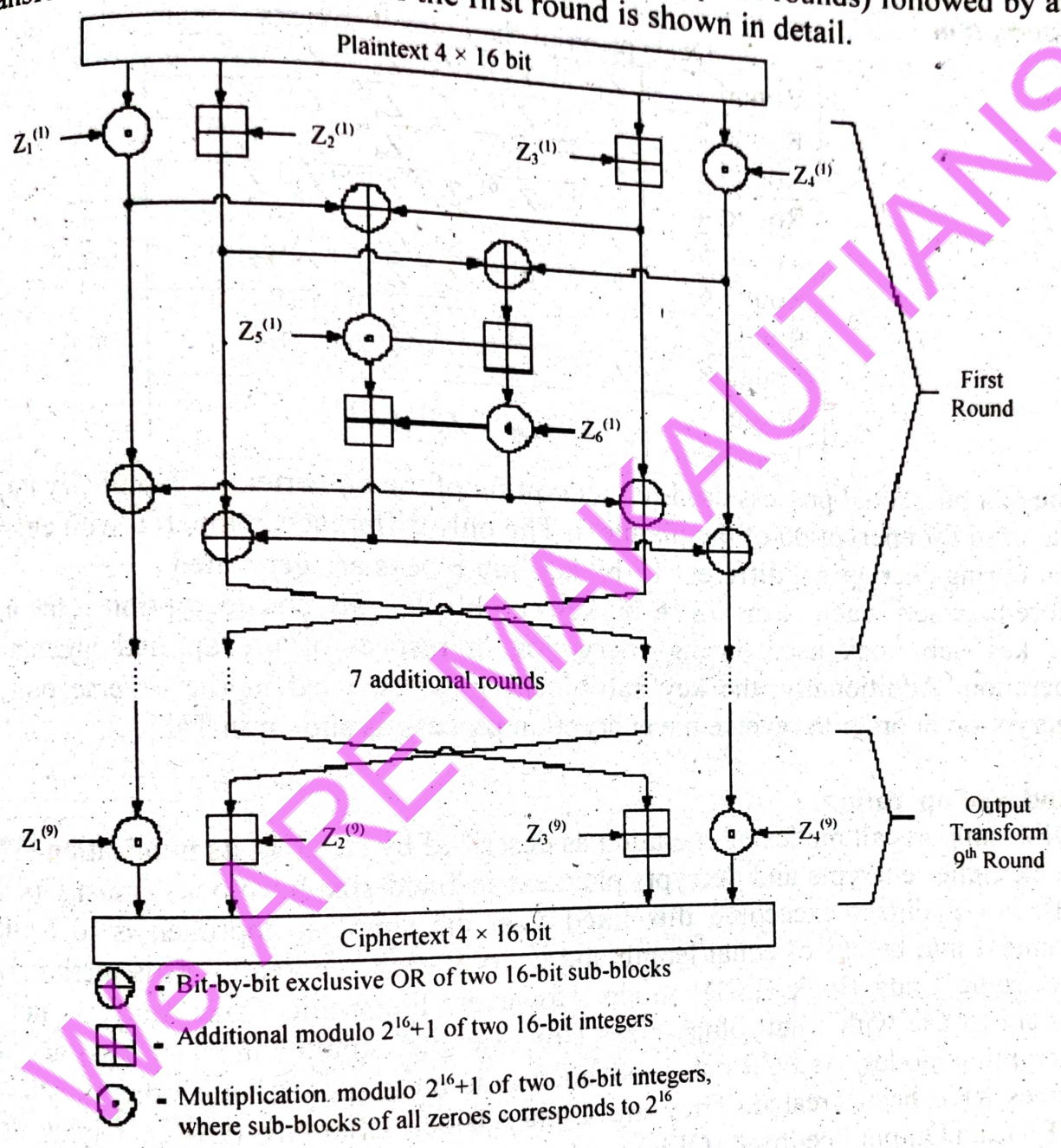


Fig: The IDEA Structure

In the first encryption round, the first four 16-bit key sub-blocks are combined with two of the 16-bit plaintext blocks using addition modulo 2^{16}, and with the other two plaintext blocks using multiplication modulo $2^{16} + 1$. The results are then processed further as shown in Figure 1, whereby two more 16-bit key sub-blocks enter the calculation and the third algebraic group operator, the bit-by-bit exclusive OR, is used. At the end of the first encryption round four 16-bit values are produced which are used as input to the second encryption round in a partially changed order. The process described above for round one is repeated in each of the subsequent 7 encryption rounds using different 16-bit key sub-blocks for each combination. During the subsequent output transformation, the four 16-bit values produced at the end of the 8th encryption round are combined with the last four

WE ARE MAKAUTIANS

of the 52 key sub-blocks using addition modulo 2^{16} and multiplication modulo $2^{16}+1$ to form the resulting four 16-bit ciphertext blocks.

Decryption

Decryption of the key sub-blocks

Round 1	$Z_1^{(9)-1}$ $-Z_2^{(9)}$ $-Z_3^{(9)}$ $Z_4^{(9)-1}$ $Z_5^{(8)}$ $Z_6^{(8)}$
Round 2	$Z_1^{(8)-1}$ $-Z_3^{(8)}$ $-Z_2^{(8)}$ $Z_4^{(8)-1}$ $Z_5^{(7)}$ $Z_6^{(7)}$
Round 3	$Z_1^{(7)-1}$ $-Z_3^{(7)}$ $-Z_2^{(7)}$ $Z_4^{(7)-1}$ $Z_5^{(6)}$ $Z_6^{(6)}$
Round 4	$Z_1^{(6)-1}$ $-Z_3^{(6)}$ $-Z_2^{(6)}$ $Z_4^{(6)-1}$ $Z_5^{(5)}$ $Z_6^{(5)}$
Round 5	$Z_1^{(5)-1}$ $-Z_3^{(5)}$ $-Z_2^{(5)}$ $Z_4^{(5)-1}$ $Z_5^{(4)}$ $Z_6^{(4)}$
Round 6	$Z_1^{(4)-1}$ $-Z_3^{(4)}$ $-Z_2^{(4)}$ $Z_4^{(4)-1}$ $Z_5^{(3)}$ $Z_6^{(3)}$
Round 7	$Z_1^{(3)-1}$ $-Z_3^{(3)}$ $-Z_2^{(3)}$ $Z_4^{(3)-1}$ $Z_5^{(2)}$ $Z_6^{(2)}$
Round 8	$Z_1^{(2)-1}$ $-Z_3^{(2)}$ $-Z_2^{(2)}$ $Z_4^{(2)-1}$ $Z_5^{(1)}$ $Z_6^{(1)}$
Output Transform	$Z_1^{(1)-1}$ $-Z_2^{(1)}$ $-Z_3^{(1)}$ $Z_4^{(1)-1}$

The computational process used for decryption of the ciphertext is essentially the same as that used for encryption of the plaintext. The only difference compared with encryption is that during decryption, different 16-bit key sub-blocks are generated.

More precisely, each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption in respect of the applied algebraic group operation. Additionally, the key sub-blocks must be used in the reverse order during decryption in order to reverse the encryption process as shown in Table 2.

Modes of operation

IDEA supports all modes of operation as described by NIST in its publication FIPS 81. A block cipher encrypts and decrypts plaintext in fixed-size-bit blocks (mostly 64 and 128 bit). For plaintext exceeding this fixed size, the simplest approach is to partition the plaintext into blocks of equal length and encrypt each separately. This method is named Electronic Code Book (ECB) mode. However, Electronic Code Book is not a good system to use with small block sizes (for example, smaller than 40 bits) and identical encryption modes. As ECB has disadvantages in most applications, other methods named modes have been created. They are Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB) modes.

2. Describe the working principle of DES algorithm for ensuring security.

[MODEL QUESTION]

Answer:

Figure below shows the sequence of events that occur during an encryption operation. DES performs an initial permutation on the entire 64 bit block of data. It is then split into 2, 32 bit sub-blocks, Li and Ri which are then passed into what is known as a round, of which there are 16 (the subscript i in Li and Ri indicates the current round). Each of the rounds are identical and the effects of increasing their number is twofold - the algorithms security is increased and its temporal efficiency decreased. Clearly these are two

WE ARE MAKAUTIANS

conflicting outcomes and a compromise must be made. For DES the number chosen was 16, probably to guarantee the elimination of any correlation between the ciphertext and either the plaintext or key6. At the end of the 16th round, the 32 bit Li and Ri output quantities are swapped to create what is known as the pre-output. This [R16, L16] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit ciphertext.

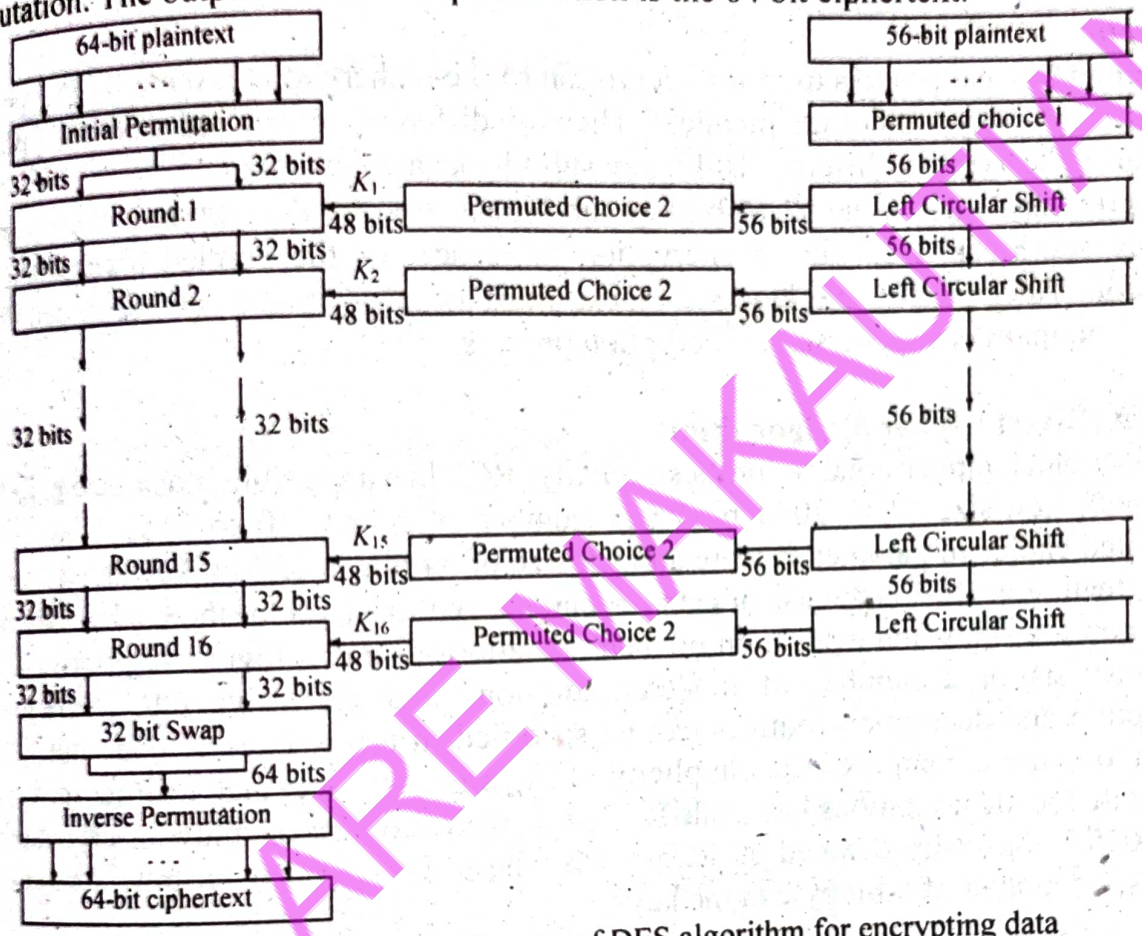


Fig: Flow diagram of DES algorithm for encrypting data

[MODEL QUESTION]

3. Write short notes on the following:

i) IDEA (International Data Encryption Algorithm) algorithm

ii) RC5 (Rivest Cipher 5) algorithm

Answer:

i) Encryption

The functional representation of the encryption process is given below. The process consists of eight identical encryption steps (known as encryption rounds) followed by an output transformation. The structure of the first round is shown in detail.

In the first encryption round, the first four 16-bit key sub-blocks are combined with two of the 16-bit plaintext blocks using addition modulo 2^{16}, and with the other two plaintext blocks using multiplication modulo $2^{16} + 1$. The results are then processed by two more 16-bit key sub-blocks enter the calculation and the third algebraic group operator, the bit-by-bit exclusive OR, is used. At the end of the first encryption round four 16-bit values are produced which are used as input to the second encryption round in a partially changed order. The process described above for round one is repeated in each of the

We ARE MAKAUTIANS

subsequent 7 encryption rounds using different 16-bit key sub-blocks for each combination. During the subsequent output transformation, the four 16-bit values produced at the end of the 8th encryption round are combined with the last four of the 52 key sub-blocks using addition modulo 2^{16} and multiplication modulo $2^{16} + 1$ to form the resulting four 16-bit ciphertext blocks.

Decryption

The computational process used for decryption of the ciphertext is essentially the same as that used for encryption of the plaintext. The only difference compared with encryption is that during decryption, different 16-bit key sub-blocks are generated.

More precisely, each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption in respect of the applied algebraic group operation. Additionally, the key sub-blocks must be used in the reverse order during decryption in order to reverse the encryption process.

ii) RC5 (Rivest Cipher 5) algorithm:

RC5 is a block cipher notable for its simplicity. RC5 has a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255). The original suggested choice of parameters were a block size of 64 bits, a 128-bit key and 12 rounds. A key feature of RC5 is the use of data-dependent rotations; one of the goals of RC5 was to prompt the study and evaluation of such operations as a cryptographic primitive. RC5 also consists of a number of modular additions and eXclusive OR (XOR)s. The encryption and decryption routines can be specified in a few lines of code but the key schedule is more complex. The simplicity of the algorithm together with the novelty of the data-dependent rotations has made RC5 an attractive object of study for cryptanalysts. The RC5 is basically denoted as RC5-w/r/b where w=word size in bits, r=number of rounds, b=number of 8-bit byte in the key.

We ARE MAKAUTIANS

ASYMMETRIC KEY ALGORITHM, DIGITAL SIGNATURE AND RSA

Multiple Choice Type Questions

1. To verify a digital signature, we need the [WBUT 2014]
   a) Sender's private key
   b) Receiver's private key
   c) sender's public key
   d) Receiver's public key

Answer: (d)

2. RSA ..... be used for digital signatures. [WBUT 2014, 2015]
   a) Must not
   b) Cannot
   c) Can
   d) Should not

Answer: (c)

3. ..... is a message digest algorithm. [WBUT 2014]
   a) DES
   b) IDEA
   c) MD5
   d) RSA

Answer: (c)

4. In asymmetric-key cryptography, how many keys are required for each communicating party? [WBUT 2015]
   a) 2
   b) 3
   c) 4
   d) 1

Answer: (a)

5. Authentication service that can be used on Windows platform is [MODEL QUESTION]
   a) DES
   b) RSA
   c) KERBEROS
   d) MD5

Answer: (c)

6. We require _____ to verify digital signature. [MODEL QUESTION]
   a) receiver's public key
   b) sender's private key
   c) receiver's private key
   d) sender's public key

Answer: (b)

Short Answer Type Questions

1. Given, 2 prime numbers p = 19, q = 31. Find out N, E, D in RSA encryption process. [WBUT 2014]

Answer:

- Choose p = 19 and q = 31
- Compute n = p * q = 19 * 31 = 589
- Compute φ(n) = (p - 1) * (q - 1) = 18 * 30 = 540
- Choose e such that 1 < e < φ(n) and e and n are coprime. Let e = 463
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 7 [(7*463) % 540 = 1]

We ARE MAKAUTIANS

- Public key is (e, n) => (463, 589)
- Private key is (d, n) => (7, 589)

2. Consider the diffie-hellman scheme with a common-prime q=11 and primitive root a = 2:
i) Show that 2 is indeed a generator
ii) If the user A has public key Ya = 9, what is A's private key?
iii) If the user B has public key Yb = 3, What is the secret key K in between A and B? **[WBUT 2014]**

Answer:
i) p=11, g=2, p-1 = 10
Let's check:
Obviously 2 and 11 are co-prime so we now need to show that 2 ^ 10 mod 11 = 1.
2^10 mod 11 does equal 1 so 2 has modulo order p-1 where p is a prime and so 2 is a primitive root of 11.

ii) q =11, n=2, Ya = 9.
Ya = (n^Xa) mod p = (2^Xa) mod 11 = 9
What power of 2 has modulo order 9 mod 11?
2^1 mod 11 = 2
2^2 mod 11 = 4
2^3 mod 11 = 8
2^4 mod 11 = 5
2^5 mod 11 = 10
2^6 mod 11 = 9
Therefore Xa = 6

iii) Now all that remains is to find the secret key K:
K = (Yb ^ Xa) mod q = 3^6 mod 11 = 3

3. What type of key is generated or exchanged by using Diffie-Hellman key exchange algorithm? Justify your answer. **[WBUT 2015]**

Answer:
Diffie-Hellman Algorithm
The Diffie-Hellman algorithm was the first public-key algorithm and is still considered one of the best. IKE uses public-key cryptography to negotiate security parameters and protect key exchanges. Specially, the Diffie-Hellman algorithm is used in the IKE negotiations to enable the two peers to agree on a shared secret by generating the key for use. This is why you will see that the Diffie-Hellman algorithm is used several times throughout the process.
In general, here is how the algorithm works: Each peer contains a private key. The Diffie-Hellman algorithm takes that private key and generates a public key. The public key is a product of the private key, but is such that the private key cannot be deduced by knowing the public key. The peers then exchange public keys, as shown in the figure below:

We ARE MAKAUTIANS

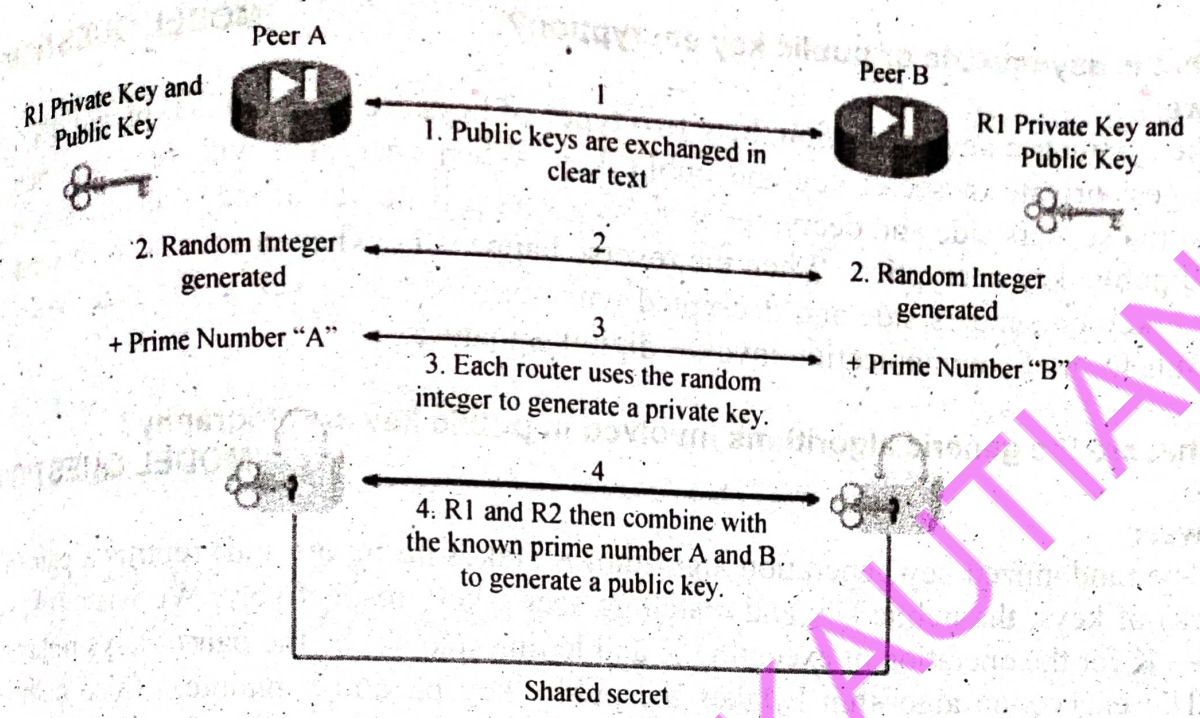


Fig: Diffie-Hellman Key Exchange

4. What are the properties that a digital signature should have?

[MODEL QUESTION]

Answer:

To summarize, digital signatures have the following properties:

- The signature can only be created by someone who knows the secret information.
- Once a signature is created, anyone can validate that the signature is associated with the individual and the document, without needing to know the secret information used to create the digital signature.
- Since the signature depends on the document, it cannot be used to validate a different document.
- It is impossible to produce a document that differs from the original document by even a single bit but for which the signature is still valid.

In this way, the digital signature replicates the desirable features of a handwritten signature, and offers even stronger forms of authentication if the proper procedures are followed in the handling of secret information. For example, handwritten signatures can be verified only by experts practicing what can only be described as an inexact science. By contrast, the mathematical procedure for verifying digital signatures can be verified by any number of independent agents, and there is no room for disagreement among these agents. The numbers are either correct or they are not.

5. How should one check that the data is untampered, error-free, unread?

[MODEL QUESTION]

Answer:

i) untampered - Hash Functions
ii) error-free - Checksums
iii) unread - Quantum tracing

WE ARE MAKAUTIANS

6. What is asymmetric or public key encryption? **[MODEL QUESTION]**

Answer:

Unlike symmetric key encryption, here two types of keys are used to encrypt and decrypt messages- private or secret key and public key. When encrypted with receivers public key at the senders side and decrypted with receivers private key at the receivers side it is called public key encryption. When the reverse happens i.e when encrypted with senders private key on senders side and decrypted with senders public key at the receivers side then this form of communication invokes digital signature.

7. What are the generic algorithms involved in public key cryptography? **[MODEL QUESTION]**

Answer:

- The randomized key generation algorithm K (takes no inputs and) returns a pair (pk, sk) of keys, the public key and matching secret key, respectively. We write (pk, sk) ← K for the operation of executing K and letting (pk, sk) be the pair of keys returned.
- The encryption algorithm E takes the public key pk and a plaintext (also called a message) M to return a value called the ciphertext. We write $C \leftarrow E_{pk}(M)$ or $C \leftarrow E(pk,M)$ for the operation of running E on inputs pk,M and letting C be the ciphertext returned.
- The deterministic decryption algorithm D takes the secret key sk and a ciphertext C to return a message M. We write $M \leftarrow D_{sk}(C)$ or $M \leftarrow D(sk,C)$.

8. What are the characteristics of public key encryption? **[MODEL QUESTION]**

Answer:

- Public Key Cryptography – One of the keys would be publicly known whereas the other would be private
- Must be computationally easy to encipher or decipher a message given the appropriate key
- Must be computationally infeasible to derive the private key from the public key
- Must be computationally infeasible to determine the private key from a chosen plaintext attack

9. Give two examples of public key encryption algorithm. **[MODEL QUESTION]**

Answer:

Diffie-Hellman and RSA are two popular public key cryptography algorithm.

Diffie-Hellman

- A pair of users generate a common key.
- To find k such that $n=g^k \bmod p$ for given n, g and prime p
- also known as Symmetric key exchange protocol

RSA – exponentiation cipher

- Two large prime numbers p and q to be chosen and n=pq computed
- totient f(n) computed
- chose an integer e < n and relatively prime to f(n)

WE ARE MAKAUTIANS

- find d such that *ed* mod f(n) = 1

10. What do you mean by key management? **[MODEL QUESTION]**

Answer:

- Refers to the distribution of cryptographic keys
- mechanisms used to bind an identity to a key
- generation and maintenance of keys
- revoking of keys

11. Name two popular Hash functions. **[MODEL QUESTION]**

Answer:

MD5 – Message Digest #5 and SHA – Secure Hash Algorithm

MD5 – Message Digest #5

- Invented by Ron Rivest (the R in RSA) of RSA Security Inc.
- MD5 computes a hash value of 128 bits (16 bytes) out of an arbitrary-sized binary document.

SHA – Secure Hash Algorithm

- Developed by the US National Institute of Standards and Technology (NIST) with the assistance of the National Security Agency (NSA).
- SHA-1 computes a hash value of 160 bits (20 bytes) out of an arbitrary-sized binary document. The algorithm is similar to MD5.
- SHA-1 is more secure than MD5 due to its increased hash size.
- An improved SHA-2 algorithm with hash sizes of 256 bits (32 bytes), 384 bits (48 bytes) and 512 bits (64 bytes) was published by NIST in October 2000 to keep up with the increased key sizes of the Advanced Encryption Standard (AES).

12. What are the modes of operation public key encryption? **[MODEL QUESTION]**

Answer:

Public-key encryption functions operate on fixed-size inputs and produce fixed-size outputs.

13. What do you mean by Symmetric & Asymmetric key Cryptography together or hybrid encryption? **[MODEL QUESTION]**

Answer:

To get the speed of symmetric key operations in open systems, key exchange protocols have been developed that initially use public-key operations to establish a shared key for a given communication session and then use that shared key (under, e.g., AES) for the remainder of the session. A simplistic example involves encrypting a large amount of data x. Given a secure public-key encryption scheme (E, D) with public key K_j for principal j, principal i can generate a new shared key k for AES and send $AES_k(x) \| E_{K_j}(k)$. Then j can decrypt k and use k to decrypt x at high speed. Key k can then be used for a session of communication between i and j.

We ARE MAKAUTIANS

14. What are the properties of Asymmetric key Cryptography? [MODEL QUESTION]

Answer:

A public-key encryption scheme (E, D) has two properties

- (Completeness) Given any message m and key pair (K, k), the encryption function and decryption function are inverses: $E_K(D_k(m)) = D_k(E_K(m)) = m$.
- (Semantic Security) For any pair of messages m and m', it is computationally hard to distinguish encryptions of m from encryptions of m', even given the public key of a principal.

15. What are the security mechanisms attempted for detection of corrupted documents and messages and protection against unauthorized modification? [MODEL QUESTION]

Answer:

Detection of corrupted documents and messages

- Detection of bit errors caused by unreliable transmission links or faulty storage media.
- Solution: Message Digest acting as a unique fingerprint for the document (similar function as CRC).

Protection against unauthorized modification

- Without protection a forger could create both an alternative document and its corresponding correct message digest.
- *Symmetric Key Solution:* Message Authentication Code (MAC) formed by using a keyed message digest function.
- *Asymmetric Key Solution:* Digital Signature formed by encrypting the message digest with the document author's private key.

16. What do you mean by data integrity? What are the algorithms involved in ensuring data integrity? [MODEL QUESTION]

Answer:

Data integrity involves checking that the received message is without data corruption like altering and tampering of the documents. Use of message digest and digital signature ensures data integrity.

17. What is authentication? What are the two methods of authentication? [MODEL QUESTION]

Answer:

Authentication is the binding of an identity to a subject. The goal of an authentication system is to ensure that entities are correctly identified. The process of authentication consists of: obtaining authentication information from an entity, analyzing the data, determining if it is associated with that entity.

Two common methods of authentication are using passwords or/and using Challenge/Response Protocol.

WeAREMAKAUTIANS

Long Answer Type Questions

1. a) Write down RSA algorithm. **[WBUT 2015]**

b) In a RSA system, the public key of a user is 17 and $N = 187$. What will be the private key of this user?

Answer:

a) RSA algorithm:

In the RSA encryption method, messages are translated into sequences of integers. This can be done by translating each letter into an integer, as is done with the Caesar cipher. These integers are grouped together to form larger integers, each representing a block of letters. The encryption proceeds by transforming the integer M, representing the plaintext (the original message) to an integer C, representing the ciphertext (the encrypted message) using the function.

$C = M^e$ **mod** n

We select 2 primes, p = 43 & q = 59 so that n = 43 · 59 = 2537, and with e = 13.

gcd (e,(p-1)(q-1) = gcd(13,42.58) = 1 (gcd = greatest common divisor)

Lets take the hypothetical message STOP, first we'll convert the letters into their numerical equivalents (position in the alphabet-1) and then group those numbers into blocks of 4.

1819 1415 = ST OP

We encrypt each block using the mapping:

$C = M^{13}$ **mod** 2537

Computations using modular multiplication show that 1819^{13} **mod** 2537 = 2081, and 1415^{13} **mod** 2537 = 2182. The encrypted message is thus 2081 2182.

RSA Decryption

The plaintext message can be quickly recovered when the decryption key d, an inverse of e modulo (p-1)(q-1) is known. (Such an inverse exists since gcd(e,(p-1)(q-1))=1). To see this, note that if d e ° 1 (mod (p-1)(q-1)), there is an integer k such that d e = 1 + k(p-1)(q-1). It follows that.

$C^d = (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)}$

By Fermat's theorem (assuming that gcd(M,p) = gcd(M,q) = 1, which holds except in rare cases, it follows that M^{p-1} ° 1 (mod p) and M^{q-1} ° 1 (mod q), consequently.

$C^d = M \cdot (M^{p-1})^{k(q-1)}$ ° M · 1 ° M (mod p)

and:-

$C^d = M \cdot (M^{q-1})^{k(p-1)}$ ° M · 1 ° M (mod q)

Since gcd(p,q) = 1, it follows that:-

C^d ° M (mod pq)

Example Decryption

Using the simple cipher above we receive the message 0981 0461, lets go about decrypting it.

n = 43·59 and e (exponent) = 13, we can work out that d = 937 is an inverse of 13 modulo 42 · 58 = 2436. We therefore use 937 as our decryption exponent, therefore.

WE ARE MAKAUTians

$P = C^{937}$ **mod** 2537
We compute 0981^{937} **mod** 2537, = 0704 and 0461^{937} **mod** 2537 = 1115. Translation reveals that this message was HELP.

b) $p = 17 \quad q = 11 \quad n = 187 \quad \phi(n) = 160$
Let us choose $\ell = 7$ since gcd(7, 160)=1
Let us complete $d : de = 1 \bmod 160$
$d = 23$ (in fact 23×7) = 161 = 1 mod 160
Public key = {7, 187}
Private key = 23

2. a) How digital signatures can be generated? **[WBUT 2015]**
b) Compare and contrast MD5 and SHA-1 algorithms.
Answer:
a) How digital signatures work
The private key of the originator is used as input to the algorithm which transforms the data being signed (or its hash value). This transformation can only be reversed, and the data decrypted and accessed, by use of the originator's public key, which is provided to the recipient(s) by the originator.

Creating a digital signature with a private key
Data encryption using asymmetric keys is an expensive operation directly proportional to the size of the data being encrypted; it potentially doubles the size of the data increasing the processing power and bandwidth required to process and transfer the data. A more efficient approach is to first use a secure cryptographic hash function (such as SHA-1) which can take large objects of varying size and produce a unique fixed-size hash value or message digest. The much smaller hash value can then be encrypted with the private key of the originator to produce the digital signature.
Having calculated the message digest this can be encrypted using the private key of the originator to produce the digital signature, as shown in the diagram below:

WE ARE MAKAUTIANS

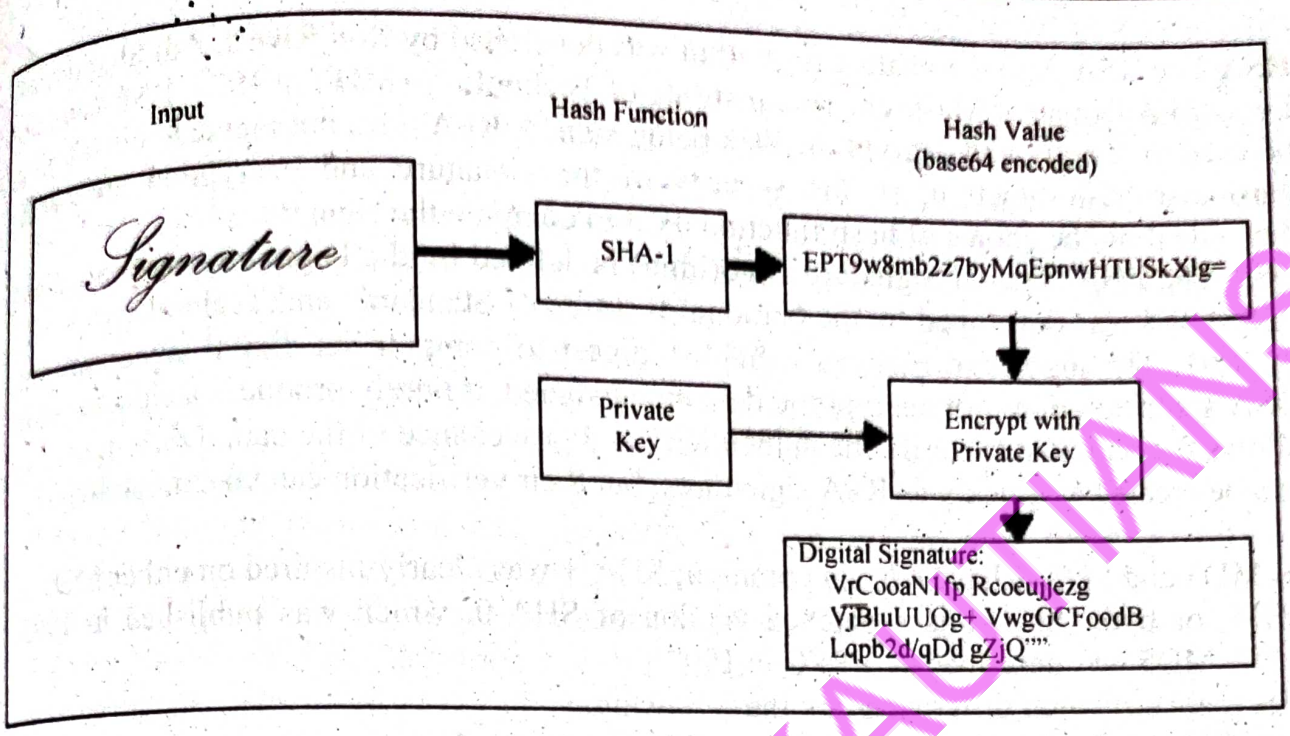


Fig: Creating a digital signature

Verifying a digital signature created with a private key

The recipient must de-crypt the digital signature using the public key of the originator and recalculate the hash value of the corresponding digital object. If the calculated hash value does not match the result of the decrypted signature, either the object has been altered since being signed, or the signature was not generated with the corresponding private key of the originator.

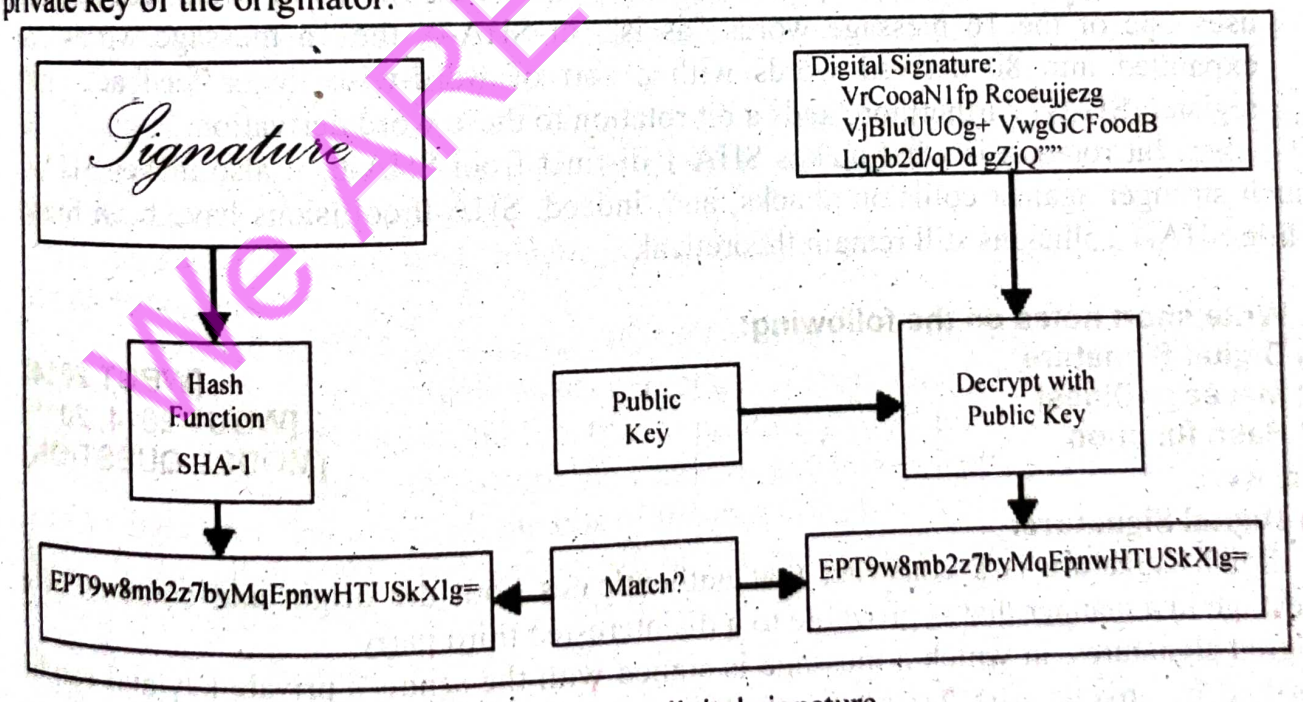


Fig: Verifying a digital signature

Digital signature algorithms

Just as there are a number of algorithms for creating hash values, there are also a number of digital signature algorithms. Two of the most commonly used are RSA and DSA.

We ARE MAKAUTIANS

RSA The RSA digital signature algorithm was developed by Ron Rivest, Adi Shamir and Leonard Adleman at Massachusetts Institute of Technology (MIT) in 1977. RSA can also be used to encrypt and decrypt the data being signed. RSA does not mandate the use of a particular hash function, so the security of the signature and encryption are partly dependent on the choice of hash function used to compute the signature.

DSA The DSA (Digital Signature Algorithm) is defined by the Digital Security Standard (DSS) and was developed by the National Institute of Standards and Technology (NIST) in 1991. The algorithm requires a SHA-1 digest to compute its digital signature. The DSA algorithm does not encrypt the data being signed, it purely produces a signature that allows the recipient to verify the authenticity and provenance of the data. DSA signatures can be created as quickly as RSA signatures, but their verification can take much longer.

b) MD5 and SHA-1 have a lot in common; SHA-1 was clearly inspired on either MD5 or MD4, or both (SHA-1 is a patched version of SHA-0, which was published in 1993, while MD5 was described as a RFC in 1992).

The main structural differences are the following:

- SHA-1 has a larger state: 160 bits vs. 128 bits.
- SHA-1 has more rounds: 80 vs. 64.
- SHA-1 rounds have an extra bit rotation and the mixing of state words is slightly different (mostly to account for the fifth word).
- Bitwise combination functions and round constants are different.
- Bit rotation counts in SHA-1 are the same for all rounds, while in MD5 each round has its own rotation count.
- The message words are pre-processed in SHA-0 and SHA-1. In MD5, each round uses one of the 16 message words "as is"; in SHA-0, the 16 message words are expanded into 80 derived words with a sort of word-wise linear feedback shift register. SHA-1 furthermore adds a bit rotation to these word derivation.

The extra bit rotation is what makes SHA-1 distinct from SHA-0; it also makes SHA-1 much stronger against collision attacks, and, indeed, SHA-0 collisions have been found while SHA-1 collisions still remain theoretical.

3. Write short notes on the following:

a) Digital Signature **[WBUT 2014]**

b) Message Digest **[WBUT 2014, 2015]**

c) Hash function **[MODEL QUESTION]**

Answer:

a) Digital Signature:

A digital signature is a construct that authenticates both the origin and contents of a message in a manner that is provable to a disinterested third party.

Digital signatures, in which a message is signed with the sender's private key and can be verified by anyone who has access to the sender's public key. This verification proves that the sender had access to the private key, and therefore is likely to be the person associated with the public key. This also ensures that the message has not been tampered,

We ARE MAKAUTIANS

as any manipulation of the message will result in changes to the encoded message digest, which otherwise remains unchanged between the sender and receiver.
Example: Think of Alice's signature on a contract with Bob. Bob not only has to know that Alice is the other signer and is signing it; he also must be able to prove to a disinterested third party (called a judge) that Alice signed it and that the contract he presents has not been altered since Alice signed it. Such a construct is called a digital signature. A digital certificate contains the digital signature of the certificate-issuing authority (CA) so that anyone can verify that the certificate is real

b) Message Digest:

The hash value represents concisely the longer message or document from which it was computed; this value is called the *message digest*. One can think of a message digest as a "digital fingerprint" of the larger document MD5 was proposed by Rivest, part of RSA Security PKCS. MD5 is 128-bit message digest function. MD5 and SHA are based on the same principles. However, MD5 may not be considered secure anymore due to its length.
Working principle of message digest function (SHA) is as follows:

1. Pad message so its length is 448 mod 512
2. Append a 64-bit length value to message
3. Initialise 5-word (160-bit) buffer (A,B,C,D,E) to (67452301,efcdab89,98badcfe,10325476,c3d2e1f0)
4. Process message in 16-word (512-bit) chunks:
5. Expand 16 words into 80 words by mixing & shifting
6. use 4 rounds of 20 bit operations on message block & buffer
7. Add output to input to form new buffer value
8. Output hash value is the final buffer value

MD5 and SHA1 are algorithms for computing a 'condensed representation' of a message or a data file. The 'condensed representation' is of fixed length and is known as a 'message digest' or 'fingerprint'.
A comparison of the two hash functions and make it clear that they have very similar design principles.
SHA-1, published in 1994, produces a 160-bit (20 byte) message digest. Although slower than MD5, this larger digest size makes it stronger against brute force attacks. SHA1 uses five rounds of an MD5 like round function to produce five 32 bit blocks. The new feature of SHA1 is an expansion step before the five rounds. It is a simple linear feedback shift register expansion that mixes all the bits of the input block.
MD5, developed in 1994, produces an 128 bit (16 byte) message digest which makes it a faster implementation than SHA-1. MD5 uses four rounds to produce four 32 bit blocks.
In both cases, the fingerprint (message digest) is also non-reversible data cannot be retrieved from the message digest, yet as stated earlier, the digest uniquely identifies the data.

c) Hash function:

A hash function H is a transformation that takes a variable-size input m and returns a fixed-size string, which is called the hash value h (that is, h = H(m)). Hash functions with

WeARE MAKAUTIANS

just this property have a variety of general computational uses, but when employed in cryptography the hash functions are usually chosen to have some additional properties.

The basic requirements for a cryptographic hash function are:

- ✓ the input can be of any length,
- ✓ the output has a fixed length,
- ✓ H(x) is relatively easy to compute for any given x ,
- ✓ H(x) is one-way,
- ✓ H(x) is collision-free.

A hash function H is said to be one-way if it is hard to invert, where "hard to invert" means that given a hash value h, it is computationally infeasible to find some input x such that H(x) = h.

If, given a message x, it is computationally infeasible to find a message y not equal to x such that H(x) = H(y) then H is said to be a weakly collision-free hash function.

A strongly collision-free hash function H is one for which it is computationally infeasible to find any two messages x and y such that H(x) = H(y).

The hash value represents concisely the longer message or document from which it was computed; one can think of a message digest as a "digital fingerprint" of the larger document. Examples of well-known hash functions are MD2 and MD5 and SHA.

4. a) In the public-key system using RSA, you intercept the cipher text CT=10 sent to a user whose public key is E=5, N=35. What is the plain text PT?
b) In an RSA system, the public key of a given user is E=31, N=3599. What is the private key of the user? **[MODEL QUESTION]**

Answer:

a) We know that the ciphertext CT = 10, and the public key PU = {e, n} = {5, 35}.

Based on Euler's Totient function, $\phi(n)$ is defined as the number of positive integers less than n and relatively prime to n [textbook: "Cryptography and Network Security", page 240]. We could find that $\phi(n) = 24$.

Now, we guess two prime numbers p and q. Let p be 5 and q be 7. All the following conditions will be satisfied based on the guess:

(1) $n = p*q = 5*7=35$

(2) $\phi(n) = (p-1)(q-1)=(5-1)(7-1)=4*6=24$

(3) $\gcd(\phi(n), e) = \gcd(24, 5) =1, 1< e < \phi(n)$

We calculate d in the next step. Based on RSA key generation algorithm,

$d \equiv e\text{-}1 \bmod \phi(n)$ which is equivalent to

$ed \equiv 1 \bmod \phi(n)$

or $ed \bmod \phi(n) =1$.

We have e = 5, $\phi(n) = 24$. So, 5d mod 24 =1, and d = 5.

Now, we find the private key PR = {d, n} = {5, 35}.

Based on RSA decryption algorithm,

$M = Cd \bmod n$

$= 105 \bmod 35$

$= 5$

WE ARE MAKAUTIANS

We also can verify the correctness by the RSA encryption algorithm as the following:

$$CT = PTe \bmod n = 55 \bmod 35 = 10$$

Therefore, we conclude that the plaintext PT is 5.

b) The private key can be written as {d, n}

To calculate d, we have to 1st calculate $\Phi(n)$

where $\Phi(n)$ is the number of prime factors of n

$e = 31$, $n = 3599$

It means that e is relatively prime to $\Phi(n)$, i.e. gcd $(\Phi(n), e) = 1$

To find $\Phi(n)$, we have to first check whether n is prime or not, and if it is not, what are the prime factors of n.

Step1: To find prime factors of n

By using trial and error we find that n is not prime and the prime factors of n are

$n = 3599 = 61 * 59$

Thus $p = 61$ and $q = 59$ are both prime numbers.

Step 2: To calculate $\Phi(n)$

Here we find the Euler's totient function written as $\Phi(n)$, where $\Phi(n)$ is the number of positive integers less than n and relatively prime to n.

It is clear that for a prime number p,

$$\Phi(p) = p-1$$

Now since we have two prime numbers p and q, with $p \neq q$, Then for $n = pq$,

$$\Phi(n) = \Phi(pq) = \Phi(p) * \Phi(q) = (p-1) * (q-1)$$

Therefore

$$\Phi(3599) = \Phi(61) * \Phi(59) = 60 * 58$$
$$= 3480$$

Step 3: Calculate d

We know that if gcd $(\Phi(n), e) = 1$, then e has a multiplicative inverse modulo $\Phi(n)$

Therefore

$$d \equiv e^{-1} \bmod \Phi(n)$$

i.e. d is multiplicative inverse of e mod $\Phi(n)$

So now we use the extended Euclid's algorithm to find the multiplicative inverse of e.

EXTENDED EUCLID $(\Phi(n), e)$

1. $(A1, A2, A3) \leftarrow (1, 0, m)$; $(B1, B2, B3) \leftarrow (0, 1, b)$
2. if $B3 = 0$ return $A3 = \gcd(\Phi(n), e)$; no inverse
3. if $B3 = 1$ return $B3 = \gcd(\Phi(n), e)$; $B2 = e^{-1} \bmod m$
4. $Q = [A3/B3]$
5. $(T1, T2, T3) \leftarrow (A1 - QB1, A2 - QB2, A3 - QB3)$
6. $(A1, A2, A3) \leftarrow (B1, B2, B3)$
7. $(B1, B2, B3) \leftarrow (T1, T2, T3)$
8. goto 2

We ARE MAKAUTIANS

Throughout the computation, the following relationships hold:

$$\Phi(n)T1 + eT2 = T3$$
$$\Phi(n)A1 + eA2 = A3$$
$$\Phi(n)B1 + eB2 = B3$$

Now we construct a multiplication table

Q	A1	A2	A3	B1	B2	B3
–	1	0	3480	0	1	31
112	0	1	31	1	–112	8
3	1	–112	8	-3	337	7
1	-3	337	7	4	–449	1

Now we need to check whether -449 is multiplicative inverse of 31 modulo 3480
Therefore

$$-449 * 31 = -13919$$
$$-13919 \bmod 3480 = -3479 \bmod 3480 = 1 \bmod 3480$$

Hence it is proved that d = –449 is multiplicative inverse of e = 31 mod $\Phi(n)$
So the private key of this user will be {–449, 3599}

5. a) With a help of diagram, briefly explain how public key cryptography works. Explain with a diagram, how the addition of a digital signature changes the process of public key cryptography.
b) Explain the concept of Confusion and Diffusion. **[MODEL QUESTION]**

Answer:

a) 1st Part:

One of the weaknesses some point out about symmetric key encryption is that two users attempting to communicate with each other need a secure way to do so; otherwise, an attacker can easily pluck the necessary data from the stream. In November 1976, a paper published in the journal IEEE Transactions on Information Theory, titled "New Directions in Cryptography," addressed this problem and offered up a solution: public-key encryption.

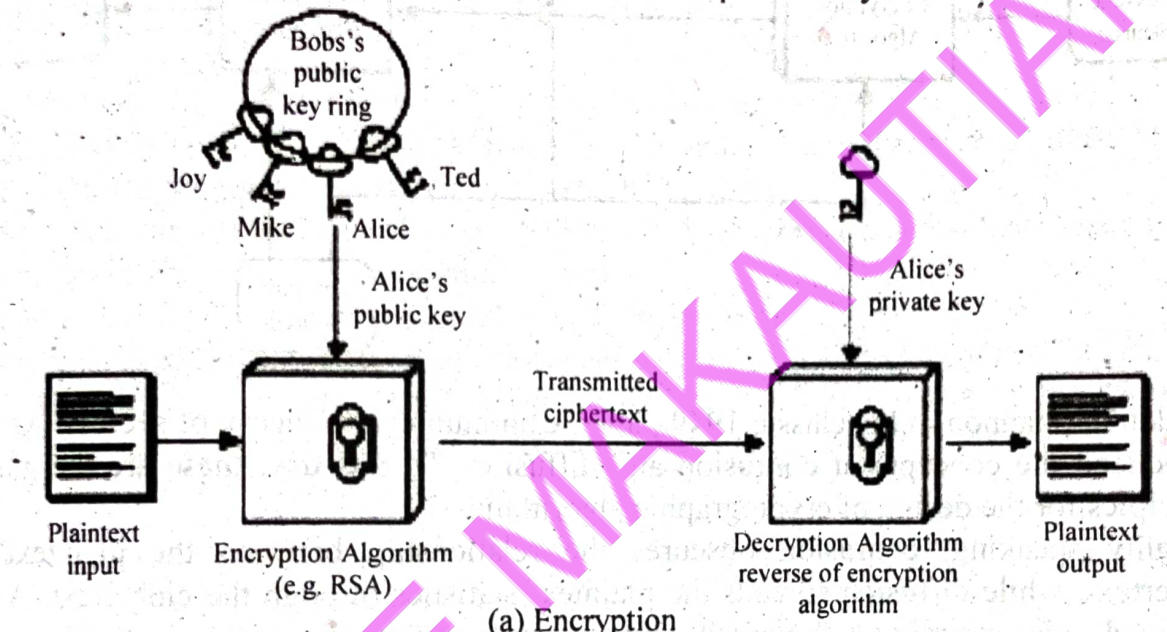
Also known as asymmetric-key encryption, public-key encryption uses two different keys at once -- a combination of a private key and a public key. The private key is known only to our computer, while the public key is given by our computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key. Although a message sent from one computer to another won't be secure since the public key used for encryption is published and available to anyone, anyone who picks it up can't read it without the private key. The key pair is based on prime numbers (numbers that only have divisors of itself and one, such as 2, 3, 5, 7, 11 and so on) of long length. This makes the system extremely secure, because there is essentially an infinite number of prime numbers available, meaning there are nearly infinite possibilities for keys. One very popular public-key encryption program is Pretty Good Privacy (PGP), which allows you to encrypt almost anything.

We ARE MAKAUTIANS

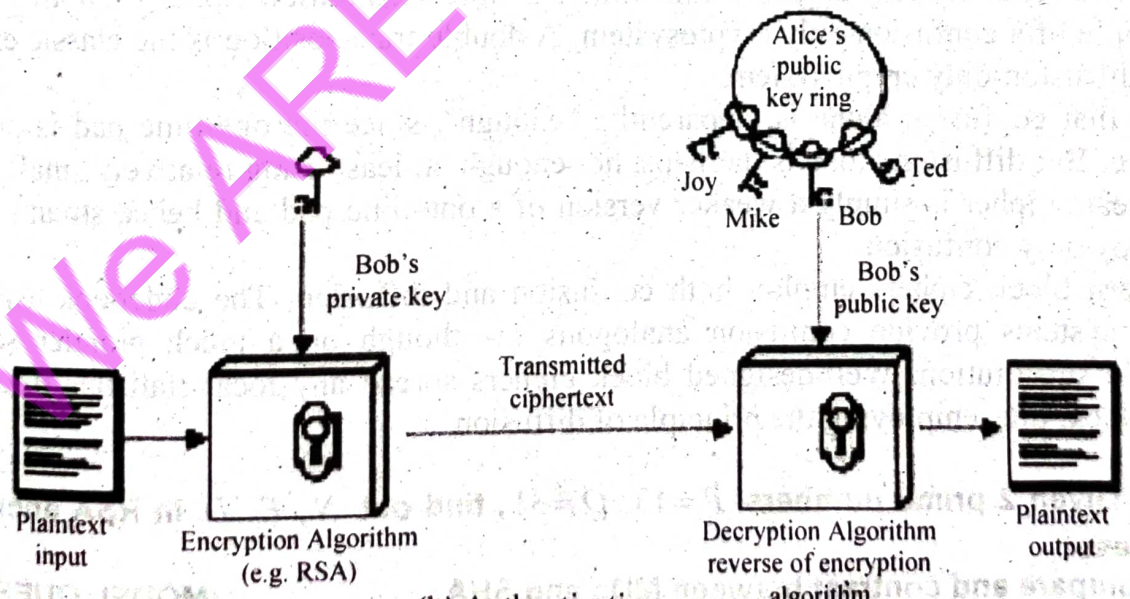
2nd Part:

The steps are:

1. Each system generates a pair of keys.
2. Each system publishes its encryption key (public key) keeping its companion key private.
3. If A wishes to send a message to B it encrypts the message using B's public key.
4. When B receives the message, it decrypts the message using its private key. No one else can decrypt the message because only B knows its private key.



(a) Encryption



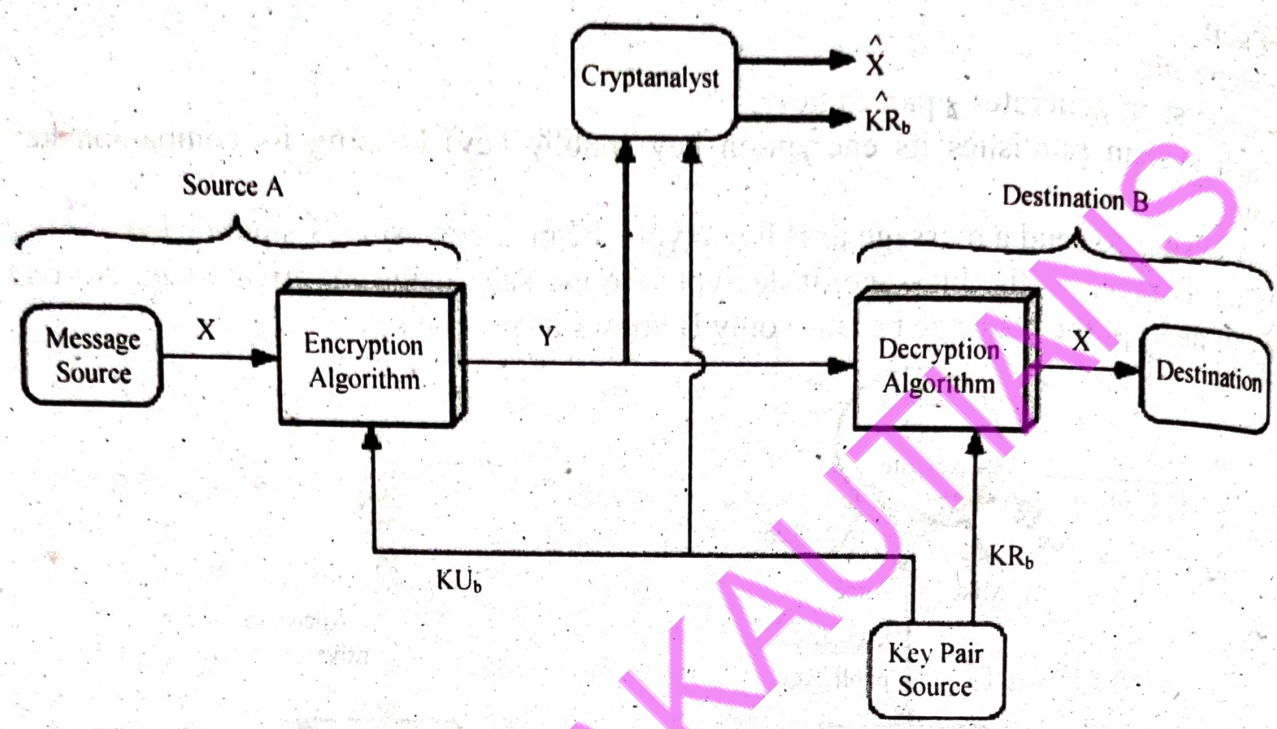
(b) Authentication

Considering P-K in more detail we have a source A that produces plaintext X destined for B. B generates a pair of keys KUb (a public key) and KRb (a private key). With X and KUb as inputs, A forms the ciphertext Y:

$Y = E_{KUb}(X)$

The intended receiver B is able to invert the transformation with his private key: $X = D_{KRb}(Y)$.

We ARE MAKAUTIANS



b) Claude Shannon in his classic 1949 paper, Communication theory of secrecy systems, introduced the concepts of confusion and diffusion. To this day, these are the guiding principles for the design of cryptographic algorithms.

Roughly speaking, confusion obscures the relationship between the plaintext and ciphertext, while diffusion spreads the plaintext statistics through the ciphertext. A one-time pad relies entirely on confusion while a simple substitution cipher is another (weak) example of a confusion-only cryptosystem. A double transposition is the classic example of a diffusion-only cryptosystem.

Note that confusion alone is, apparently, "enough", since the one-time pad is provably secure. But diffusion alone is, perhaps, not enough, at least using relatively small blocks. A stream cipher is simply a weaker version of a one-time pad and hence stream ciphers employ only confusion.

Modern block ciphers employ both confusion and diffusion. The codebook aspects of such systems provide confusion analogous to---though on a much grander scale---a simple substitution. Well-designed block ciphers spread any local statistics throughout the block, thus employing the principle of diffusion.

6. a) Given 2 prime numbers $P = 13$, $Q = 31$, find out N, E, D in RSA encryption process.

b) Compare and contrast between MD5 and SHA. **[MODEL QUESTION]**

Answer:

a) Choose p = 13 and q = 31

Compute n = p * q = 13 * 31 = 403

Compute φ(n) = (p - 1) * (q - 1) = 12 * 30 = 360

Choose e such that 1 < e < φ(n) and e and n are coprime. Let e = 7

Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 103 [(103 * 7) % 360 = 1]

WE ARE MAKAUTians

Public key is (e, n) => (7, 403)
Private key is (d, n) => (103, 403)

b) MD5 – Message Digest #5 and SHA – Secure Hash Algorithm

MD5 – Message Digest #5

- Invented by Ron Rivest (the R in RSA) of RSA Security Inc.
- MD5 computes a hash value of 128 bits (16 bytes) out of an arbitrary-sized binary document.

SHA – Secure Hash Algorithm

- Developed by the US National Institute of Standards and Technology (NIST) with the assistance of the National Security Agency (NSA).
- SHA-1 computes a hash value of 160 bits (20 bytes) out of an arbitrary-sized binary document. The algorithm is similar to MD5.
- SHA-1 is more secure than MD5 due to its increased hash size.
- An improved SHA-2 algorithm with hash sizes of 256 bits (32 bytes), 384 bits (48 bytes) and 512 bits (64 bytes) was published by NIST in October 2000 to keep up with the increased key sizes of the Advanced Encryption Standard (AES).

We ARE MAKAUTIANS

INTERNET SECURITY PROTOCOLS, USER AUTHENTICATION

Multiple Choice Type Questions

1. Biometric authentication works on the basic of [WBUT 2014]
   a) Human characteristics
   b) Passwords
   c) Smart cards
   d) PINs

Answer: (a)

2. ..... forms the basic for the randomness of an authentication token. [WBUT 2014]
   a) Password
   b) Seed
   c) User id
   d) Message digest

Answer: (b)

3. SSL layer is located between [MODEL QUESTION]
   a) transport layer, network layer
   b) application layer, transport layer
   c) data link layer, physical layer
   d) network layer, data link layer

Answer: (b)

4. IPsec services are available in _____ layer. [MODEL QUESTION]
   a) Application
   b) Data link
   c) Network
   d) Transport

Answer: (c)

Short Answer Type Questions

1. What do you mean by 2-factor authentication? [WBUT 2014].

Answer:

Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. In this context, the two factors involved are sometimes spoken of as something we have and something we know. A common example of two-factor authentication is a bank card: the card itself is the physical item and the personal identification number (PIN) is the data that goes with it. According to proponents, two-factor authentication could drastically reduce the incidence of online identity theft, phishing expeditions, and other online fraud, because the victim's password would no longer be enough to give a thief access to their information. Opponents argue (among other things) that, should a thief have access to your computer, he can boot up in safe mode, bypass the physical authentication processes, scan your system for all passwords and enter the data manually, thus -- at least in this situation -- making two-factor authentication no more secure than the use of a password alone.

We ARE MAKAUTIANS

2. Describe the functioning of an MAC? **[WBUT 2014]**

Answer:

While **message authentication code** (MAC) functions are similar to cryptographic hash functions, they possess different security requirements. To be considered secure, a MAC function must resist existential forgery under chosen-plaintext attacks. This means that even if an attacker has access to an oracle which possesses the secret key and generates MACs for messages of the attacker's choosing, the attacker cannot guess the MAC for other messages (which were not used to query the oracle) without performing infeasible amounts of computation.

MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages. In contrast, a digital signature is generated using the private key of a key pair, which is public-key cryptography. Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer non-repudiation.

However, non-repudiation can be provided by systems that securely bind key usage information to the MAC key; the same key is in possession of two people, but one has a copy of the key that can be used for MAC generation while the other has a copy of the key in a hardware security module that only permits MAC verification. This is commonly done in the finance industry.

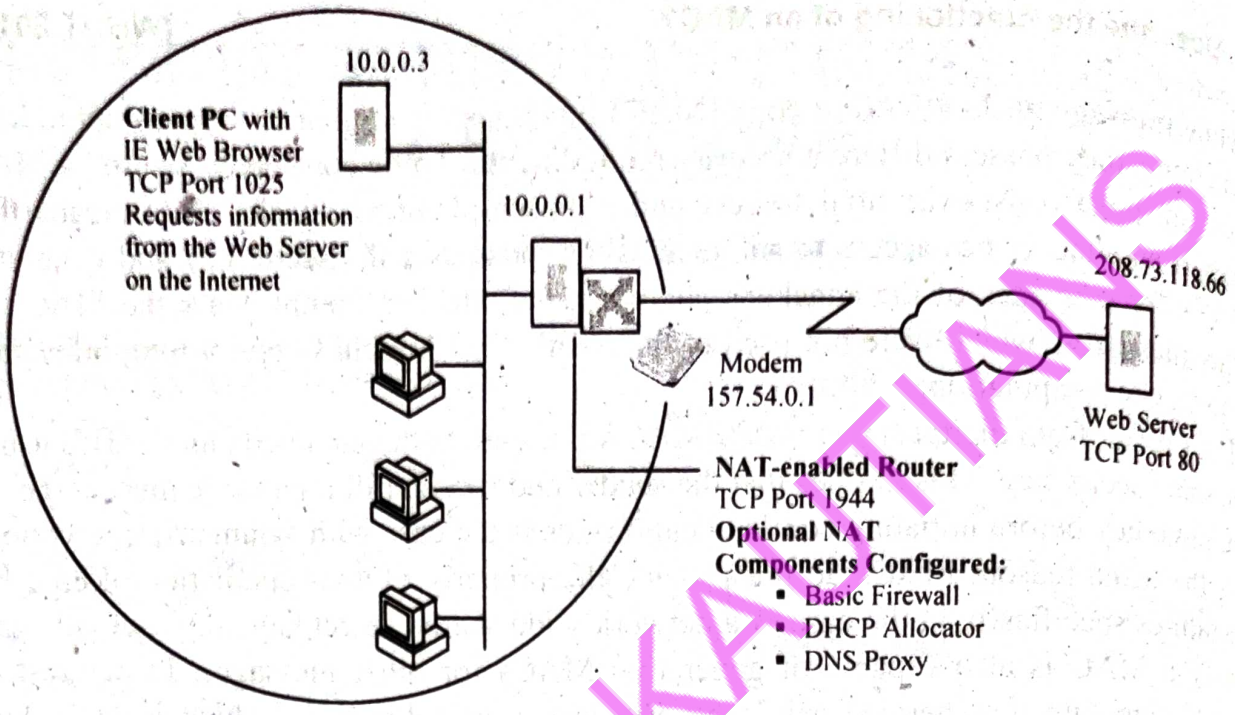
3. Explain how NAT works with an example. **[WBUT 2014]**

Answer:

The following figure shows an example of a single-subnet private network that uses a Routing and Remote Access NAT-enabled router to provide access to the Internet. Computers on the private network have a private IPv4 address, except for the router, which has both a private and a public address. The Web server, like any computer on the Internet, has a public IPv4 address.

Client on a Private Network Behind a Routing and Remote Access NAT Accessing a Resource over the Internet.

WE ARE MAKAUTIANS



The following table describes each component shown in the preceding figure.

Component	Description
Client PCs	Each client has a private IPv4 address configured on its network adapter. Clients need only a Web browser and access to a NAT-enabled router to be able to access the Web server across the Internet.
Routing and Remote Access NAT-enabled router	The NAT-enabled router has a private IP v4 address configured on its private interface, and a public IPv4 address configured on its Internet interface (in this example, a dial-up modem). The router has the optional Basic Firewall, DHCP allocator, and DNS proxy NAT components enabled. For more information, see "Optional NAT Subsystems." For a larger network, an administrator might also configure a more sophisticated firewall in addition to using Basic Firewall to protect the Internet interface of the NAT-enabled router and might use a DHCP server (required if the network has more than one segment) and a DNS server.
Web server	A Web server on the Internet provides resources needed by the client computers on the private network. Like all computers on the Internet, it has a public IPv4 address.

We ARE MAKAUTIANS

SSL - Secure Socket Layer

4. Differentiate between transport and tunnel modes of operation of IPsec. **[WBUT 2015]**

Answer:

- Tunnel mode encapsulates the whole IP packet by either encrypting, authenticating or most likely doing both. Tunnel mode will encapsulate our packets with IPSec headers and trailers.
- Transport mode can be used to protect IPsec peers traffic that they exchange and generate by themselves. This means that if we configure transport mode on some tunnel interface it will only be used when the traffic to be protected has the same IP addresses as the IPSec peers. Though it could also be encapsulated in tunnel mode like everything else but here is an interesting concept.
- Transport mode having Larger MTU than Tunnel mode
- Transport mode Requires IPsec to be implemented on the IPS entities whereas Tunnel mode Don't have to implement IPsec on the IPS entity
- Traversing NATs is easier in tunnel mode than transport mode

5. How is S-HTTP different from SSL? **[WBUT 2015]**

Answer:

Secure Sockets Layer (SSL) and Secure Hypertext Transport Protocol (S-HTTP) allow for the exchange of multiple messages between two processes.

The main difference between these protocols and PGP and PEM is that SSL and S-HTTP use a session model, and thus the security mechanisms and parameters used during a session can be negotiated. This allows the degree and kind of security to be varied according to such factors as the nature of the data being exchanged and the vulnerabilities of the underlying communication media. SSL and S-HTTP were designed primarily for WWW-based commerce.

In terms of implementation, SSL fits between the session and transport layers, and is implemented as a replacement for the sockets API to be used by applications requiring secure communications. S-HTTP, on the other hand, is similar to PEM in terms of implementation - its data are passed in named text fields in the HTTP header.

6. a) Why is the SSL layer positioned between the application layer and transport layer?

b) What are the problems associated with clear text password? **[WBUT 2015]**

Answer:

a) Because of its position, SSL gives the client machines the ability to selectively apply security protection on individual applications, rather than set forth encryption on an entire group of applications. The procedure can be done without concerning Layer 3, the network layer. For these reasons, when SSL is used for encrypting network traffic, only the application layer data is actually encrypted. This differs from, say, the IPsec protocol, which operates at the network layer and encrypts all traffic data right down to the IP layer.

WE ARE MAKAUTIANS

b) The problem happens in at least five different areas:
Clear text password **during input:** This problem occurs when end users type passwords and those passwords remain visible on the screen after being typed.
Clear text password **during management:** This problem occurs when an operator pulls up a connection profile and can read the password off the profile when he/she really only should be using an existing profile.
Clear text password **during storage:** This problem happens when configuration files, customer profiles or FTP scripts are written to disk and no encryption is used to protect the stored data.
Clear text password **in trace logs:** This problem occurs when passwords are written into trace logs.
Clear text password **on the wire:** This problem occurs when passwords are sent across a network.

7. What are authentication tokens? **[MODEL QUESTION]**

Answer:
Tokens are either physical or digital entities given to the user by the server system in exchange of their username and password, which helps a user to access resources multiple times without requiring usernames or password pair possible through out the entire session of communication.
Example of a physical token is smart card. In Kerberos authentication tokens are used.

8. Name are the different Internet security protocols. **[MODEL QUESTION]**

Answer:

- Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security for communications. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end.
- TLS allows client/server applications to communicate in a way designed to prevent eavesdropping and tampering.
- TLS provides endpoint authentication and communications confidentiality using cryptography.

9. What is the purpose of challenge/ response method in authentication? **[MODEL QUESTION]**

Answer:
Passwords have the fundamental problem that they are reusable. If an attacker sees a password, she can later replay the password. The system cannot distinguish between the attacker and the legitimate user, and allows access. An alternative is to authenticate in such a way that the transmitted password changes each time. Then, if an attacker replays a previously used password, the system will reject it. Let user U desire to authenticate himself to system S. Let U and S have an agreed-on secret function f. A challenge-response authentication system is one in which S sends a random message m (the

We ARE MAKAUTIANS

challenge) to U, and U replies with the transformation r = f(m) (the response). S validates r by computing it separately.

10. What is the common way to ensure authentication? **[MODEL QUESTION]**

Answer:

Passwords are an example of an authentication mechanism based on what people know: the user supplies a password, and the computer validates it. If the password is the one associated with the user, that user's identity is authenticated. If not, the password is rejected and the authentication fails.

11. What are the requirements of authentication? **[MODEL QUESTION]**

Answer:

- set *A* of specific (authentication) information from an entity
- Set *C* of complementary information stored with the system and used for validation
- Set *F* of complementation functions that generate the complementary information
- Set *L* of authentication functions that verify identity
- Set *S* of selection functions that enable an entity to create or alter the authentication and complementary information

12. What are the goals of password protected authentication system? **[MODEL QUESTION]**

Answer:

The goal of an authentication system is to ensure that entities are correctly identified. The goal is to find an $a \hat{I} A$ such that, for $f \hat{I} F$, $f(a)=c \hat{I} C$ and c is associated with a particular entity.

Long Answer Type Questions

1. Write short note Biometric Authentication. **[WBUT 2015]**

Answer:

Biometric authentication systems compare the current biometric data capture to stored, confirmed authentic data in a database. If both samples of the biometric data match, authentication is confirmed and access is granted. The process is sometimes part of a multifactor authentication system. For example, a smartphone user might log on with his personal identification number (PIN) and then provide an iris scan to complete the authentication process. Different mechanisms by which biometric can be included in cryptography:

- Fingerprints
  - May be scanned optically
  - A capacitative technique uses the differences in electrical charges of the whorls on the finger. The data is converted into a graph. The problem of determining matches is basically similar to the classical graph isomorphism.

We ARE MAKAUTIANS

- Voices
  - Authentication by voice involves recognition of a speaker's voice characteristics or verbal information verification. The first one uses statistical techniques to test the hypothesis that the speaker's identity is as claimed. The other one deals with the contents of utterances.
  - The difference is that the speaker verification techniques are speaker dependent whereas verbal information verification techniques are speaker-independent.
- Eyes
  - Authentication by eye characteristics uses the iris and the retina. Patterns within the iris are unique with each person. Retinal scans rely on the uniqueness of the patterns made by blood vessels at the back of the eye.
- Faces
  - Face recognition consists of various steps starting with the location of the face. This requires placing the face in a predetermined position. Techniques include neural networks and templates.
- Keystrokes
  - Keystroke dynamics requires a signature based on keystroke intervals, keystroke pressure, keystroke duration and the position of the stroke in the key. This signature is believed to be unique.

2. What do you mean by network security explain with a suitable model.
[MODEL QUESTION]

Answer:
Each layer of the NSM is built upon the layer below it, much like the OSI model, if one layer fails all layers above it will fail as well. We will look at the NSM versus an inverted OSI model as shown in figure below to show how each model relates and differs.

Network Security Model (NSM)	OSI Model (inverted)
Physical	Physical
VLAN	Data Link
ACL	Network
Software	Transport
user	Session
Administration	Presentation
IT Department	Application

The first layer is the physical layer from the NSM and the physical layer from the OSI model. Both work with the physical aspects of the network. The physical layer from the NSM deals with physical securities where the physical layer from OSI deals with physical network connections. Both layers are very self explanatory and very easy to deal with.

The second layer is the VLAN layer from the NSM and the data link layer from the OSI model. Both work similarly by dealing with MAC addressing and VLANs. The VLAN

WE ARE MAKAUTIANS

layer from the NSM deals with VLAN segmentation. This splits LAN's across switches and segments based on the data link layer from OSI model which covers MAC addressing.

The third layer is the ACL layer from the NSM and the network layer from the OSI model. Both work similarly by dealing with IP addressing and LAN's. The ACL layer from the NSM deals with ACL implementation which is used to allow or deny access based on the network layer from the OSI model which covers IP addressing.

The fourth layer is the software layer from the NSM and the transport layer from the OSI model. Both deal with the actual connection on the network from host to host. The software layer from the NSM deals with the software and the patches that allow the software to not be exploited while the transport layer from the OSI model describes the connection between the both ends of the software connection.

The fifth layer is the user layer from the NSM and the session layer from the OSI model. Both deal directly with the local host where the user layer from the NSM deals directly with the user who is able to utilize that local machine. The Session layer from the OSI model deals directly with communication on that local machine.

The sixth layer is the administrative layer from the NSM and the presentation layer from the OSI model. Both deal with administrative functions. The administrative layer deals with the administrative users who have the ability to direct users and the presentation layer deals with how the data is directed.

The seventh and final layer is the IT department layer from the NSM and the application layer from the OSI model. The IT department layer deals directly with the maintenance of all layers and making sure that the entire network works correctly from NSM model and all layers of the OSI model. The application layer from the OSI model deals with the actual display of the data.

We ARE MAKAUTIANS

3. a) Why is the SSL layer positioned between Application layer and Transport layer?

b) Name the four key steps in the creation of a Digital certificate. How is SHTTP different from SSL?

c) What are the problems associated with clear text passwords?

[MODEL QUESTION]

Answer:

a) At the receiver's end, the process happens pretty similar to how it happens in the case of a normal TCP/IP connection, until it reaches the new SSL layer. The SSL layer at the receiver's end removes the SSL Header (SH), decrypts the encrypted data and gives the plain text data back to the application layer of the receiving computer.

Thus, only the application layer data is encrypted by SSL. The lower layer headers are not encrypted. This is quite obvious; if SSL has to encrypt all the headers, it must be positioned below the data link layer. That would serve no purpose at all. in fact, it would lead to problems. If SSL encrypted all the lower layer headers, even the IP and physical address of the computers (sender, receiver and intermediate nodes) would be encrypted,

and become unreadable. Thus, what to deliver the packets would be a big question. To understand the problem, imagine what would happen if we put the address of the sender and the receiver of a letter inside the envelope! Clearly, the postal service would not know where to send the letters! This is also why there is no point in encrypting the lower layer headers. Therefore, SSL is required between the application and the transport layers.

b) 1st Part:
Digital certificate is created outside of the IP-Protector application. Then, a copy of the certificate and private key is exported for access by IP-Protector software.

Steps:
1. Creating our private signing key and certificate
   - Vendors that provide CA services
2. Exporting your certificate for access by IP-Protector
3. Recording key storage location information in IP-Protector
4. Accessing the private key to create a signature

Step 1. Creating our private signing key and requesting a public key certificate
Several vendors are listed below that provide signing certificates (public and private keys) that can be used in the IP-Protector application.
There are several techniques for creating key-pairs and certificates. Each of the vendor's web sites below will describe their unique process for creating our keys and their free trials. For example, our organization may have a defined process for creating signing certificates. The IP-Protector only requires that the certificate key-pair be stored in a IETF standard PKCS #12 record.

Step 2. Exporting your certificate for access by IP Protector
The process of exporting our certificate is identical to making a backup copy of our digital certificate. There are two decisions that we make during this process:
1. Where to store the certificate file? We suggest that we put the copy of the certificate on a removable disk like a thumb drive. The certificate file is encrypted and could be stored anywhere on our computer.
2. The password we use to protect the certificate should be difficult to guess. It should include a combination of letters and numbers and longer than 10 characters. The security of your signing certificate is only as good as the password we choose.

Step 3. Recording key storage location information in IP-Protector
This is a one-time setup task to describe where the signing key is stored. Each time we create a signature, the software will need to access this storage location and will ask us for password. During this step, the signing key file is not opened or read.

WE ARE MAKAUTIANS

Step 4. Accessing the private key to create a signature

The private key is stored inside the computer file you specified in the previous step. The private key can be accessed only by providing your password. Using your password, the private key is retrieved from the file and used to calculate your signature. The signature calculation is done inside the IP-Protector software.

2nd Part:

The main difference between the protocols is the layer at which they operate. SSL operates at the transport layer and mimics the "socket library," while S-HTTP operates at the application layer. Encryption of the transport layer allows SSL to be application-independent, while S-HTTP is limited to the specific software implementing it. The protocols adopt different philosophies towards encryption as well, with SSL encrypting the entire communications channel and S-HTTP encrypting each message independently. S-HTTP allows a user to produce digital signatures on any messages (not just specific messages during an authentication protocol), a feature SSL lacks.

c) When a password is transmitted in clear text, it is vulnerable in many ways:

1. The password is available on the wire. As the password is transmitted over the wire, tools such as packet sniffers or network analyzers can easily monitor the traffic and intercept passwords as they're sent between computers.
2. The password is available in browsing history. Most web browsers provide 'back' navigation to previous pages, with content locally cached for performance as well as ease of use for the user. These pages are stored in memory and are relatively easy to examine.
3. The password is readable on web proxies. Many larger corporations, as well as internet service providers, offer web proxies to allow faster downloads as well as some level of anonymity for web users.

4. a) What are the different sub-protocols defined by SSL? Explain one of them.
b) How can a Digital Certificate be verified? **[MODEL QUESTION]**

Answer:

a) 1st part:

Different sub-protocols defined by SSL:

Handshake: This sub-protocol negotiates session information between the client and the server. The session information includes the session ID, the compression algorithm to be used, and a shared secret used to generate keys.

Change Cipher Spec: This sub-protocol consists of a single message to tell the other party in the SSL session, who is known as the peer, that the sender wants to change to a new set of encryption keys. The keys are computed from the information that is exchanged by the Handshake sub-protocol.

We ARE MAKAUTIANS

Alert: This sub-protocol generates error messages as well as status alerts. Alerts are commonly sent when the connection is closed, an invalid message is received, a message cannot be decrypted or the user cancels the operation.

2nd part:

SSL handshake protocol is very effective for clients and server complete the mutual authentication, the main process is as follows:

(1) the client's browser to the server sending the client SSL protocol version number, the type of encryption algorithm to generate random numbers, and other communications between servers and clients all the information needed.

(2) SSL server sent to the client protocol version number, the type of encryption algorithm, random number and other relevant information to the client while the server will send its own certificate.

(3) customers using the server information transfer over the legitimacy of the authentication server, the server's legitimacy, including: the certificate is expired, the CA issued the server certificate is reliable, the public key of the certificate issuer server certificate can correctly solve the "issuer digital signature ", the server certificate on the domain name is the actual domain name and server match. If the legitimacy of verification does not pass, communication will be disconnected; if legitimacy is validated, will continue to the fourth step.

(4) client generates a random back communications for the "symmetric key", and then use the server's public key (the server's public key from the steps of the server's certificate (2) obtained) for its encryption, and then encrypted the "pre-primary password "pass the server.

(5) If the server requires a client's identity authentication (Zai handshake Zhongwei optional), the user can create a Sui Jishu and its Jinxing Shujuqianming to incorporate the Han You signed random number and the customer had their own certificates, and Jia Mi's "pre-primary password "pass with the server.

(6) If the server requires client authentication, the server must verify client certificate and the signature of random numbers of legitimacy, the legitimacy of the specific validation process includes: customers use the date the certificate is valid, the CA certificates to provide customers with the reliability issue of CA, client certificate public key can correctly solve the issue of CA's digital signature, check whether the client certificate in the certificate revocation list (CRL) in. If you do not pass inspection, communication immediately interrupted; If it is validated, the server will be encrypted with their private key unlock the "pre-master password" and then performs a series of steps to produce the primary communication code (the client will also be produced by the same method the same main communication password).

(7) server and client with the same master password that is the "call code", a symmetric key for the SSL protocol for secure data communications encryption communication. SSL communications at the same time to complete the process of data communication but also the integrity of data communications to prevent any changes.

WE ARE MAKAUTIANS

(8) client send a message to the server, specify the data communication will be used later in step (7) of the master password for the symmetric key, also informed the process server hands the client end.
(9) server send a message to the client, specify the data communication will be used later in step (7) of the master password for the symmetric key, notify the client server handshake process is completed.
(10) SSL handshake part of the end, SSL secure channel for data communications, customers and the server to start using the same symmetric key for data communication, and to communicate the integrity of the test.

b) To verify the identity of people and organizations on the Web and to ensure content integrity, Internet Explorer uses industry-standard X.509 v3 digital certificates. Certificates are electronic credentials that bind the identity of the certificate owner to a pair (public and private) of electronic keys that can be used to encrypt and sign information digitally. These electronic credentials assure that the keys actually belong to the person or organization specified. Messages can be encrypted with either the public or the private key and then decrypted with the other key.

Each certificate contains at least the following information:

- Owner's public key
- Owner's name or alias
- Expiration date of the certificate
- Serial number of the certificate
- Name of the organization that issued the certificate
- Digital signature of the organization that issued the certificate

Certificates can also contain other user-supplied information, including a postal address, an e-mail address, and basic registration information, such as the country or region, postal code, age, and gender of the user.
Certificates form the basis for secure communication and client and server authentication on the Web. We can use certificates to do the following:

- Verify the identity of clients and servers on the Web.
- Encrypt channels to provide secure communication between clients and servers.
- Encrypt messages for secure Internet e-mail communication.
- Verify the sender's identity for Internet e-mail messages.

Put your digital signature on executable code that users can download from the Web.
Verify the source and integrity of signed executable code that users can download from the Web.

WE ARE MAKAUTIANS

5. Write short notes on the following: **[MODEL QUESTION]**

a) Kerberos

b) Secure Electronic Transaction (SET)

c) Ipsec

Answer:

a) Kerberos:

Kerberos is a secure method for authenticating a request for a service in a computer network. Kerberos was developed in the Athena Project at the Massachusetts Institute of Technology (MIT). The name is taken from Greek mythology; Kerberos was a three-headed dog who guarded the gates of Hades. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server. The user's password does not have to pass through the network. A version of Kerberos (client and server) can be downloaded from MIT or we can buy a commercial version.

Briefly and approximately, here's how Kerberos works:

1. Suppose we want to access a server on another computer (which we may get to by sending a Telnet or similar login request). We know that this server requires a Kerberos "ticket" before it will honor our request.
2. To get our ticket, we first request authentication from the Authentication Server (AS). The Authentication Server creates a "session key" (which is also an encryption key) basing it on our password (which it can get from our user name) and a random value that represents the requested service. The session key is effectively a "ticket-granting ticket."
3. We next send our ticket-granting ticket to a ticket-granting server (TGS). The TGS may be physically the same server as the Authentication Server, but it's now performing a different service. The TGS returns the ticket that can be sent to the server for the requested service.
4. The service either rejects the ticket or accepts it and performs the service.
5. Because the ticket we received from the TGS is time-stamped, it allows us to make additional requests using the same ticket within a certain time period (typically, eight hours) without having to be reauthenticated. Making the ticket valid for a limited time period make it less likely that someone else will be able to use it later.

b) Secure Electronic Transaction:

Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. It was supported initially by Mastercard, Visa, Microsoft, Netscape, and others. With SET, a user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and confidentiality. SET makes use of Netscape's Secure Sockets Layer (SSL), Microsoft's Secure Transaction Technology (STT), and Terisa System's

WeARE MAKAUTIANS

Secure Hypertext Transfer Protocol (S-HTTP). SET uses some but not all aspects of a public key infrastructure (PKI).Here's how SET works:

Assume that a customer has a SET-enabled browser such as Netscape or Microsoft's Internet Explorer and that the transaction provider (bank, store, etc.) has a SET-enabled server.

1. The customer opens a Mastercard or Visa bank account. Any issuer of a credit card is some kind of bank.
2. The customer receives a digital certificate. This electronic file functions as a credit card for online purchases or other transactions. It includes a public key with an expiration date. It has been through a digital switch to the bank to ensure its validity.
3. Third-party merchants also receive certificates from the bank. These certificates include the merchant's public key and the bank's public key.
4. The customer places an order over a Web page, by phone, or some other means.
5. The customer's browser receives and confirms from the merchant's certificate that the merchant is valid.
6. The browser sends the order information. This message is encrypted with the merchant's public key, the payment information, which is encrypted with the bank's public key (which can't be read by the merchant), and information that ensures the payment can only be used with this particular order.
7. The merchant verifies the customer by checking the digital signature on the customer's certificate. This may be done by referring the certificate to the bank or to a third-party verifier.
8. The merchant sends the order message along to the bank. This includes the bank's public key, the customer's payment information (which the merchant can't decode), and the merchant's certificate.
9. The bank verifies the merchant and the message. The bank uses the digital signature on the certificate with the message and verifies the payment part of the message.
10. The bank digitally signs and sends authorization to the merchant, who can then fill the order.

c) Ipsec:

IPSec, is a framework of open standards (from IETF) that define policies for secure communication in a network. In addition, these standards also describe how to enforce these policies.

Using IPSec, participating peers (computers or machines) can achieve data confidentiality, data integrity, and data authentication at the network layer (i.e. Layer 3 of the Open Systems Interconnection 7-layer networking model). RFC 2401 specifies the base architecture for IPsec compliant systems.

We ARE MAKAUTIANS

This RFC says that "the goal of the architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments." See also RFC 2402, RFC 2406 and RFC 2407 for more details on IPSec.

The main purpose of IPSec is to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. It offers various security services at the IP layer and therefore, offers protection at this (i.e. IP) and higher layers. These security services are, for example, access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality.

IPSec has two different modes: Transport mode (host-to-host) and Tunnel Mode (Gateway-to-Gateway or Gateway-to-host). In transport mode, the payload is encapsulated (header is left intact) and the end-host (to which, the IP packet is addressed) decapsulates the packet. In the tunnel mode, the IP packet is entirely encapsulated (with a new header). The host (or gateway), specified in the new IP header, decapsulates the packet. Note that, in tunnel mode, there is no need for client software to run on the gateway and the communication between client systems and gateways are not protected.

IPSec standard supports the following features:

- AH (Authentication Header) that provides authenticity guarantee for transported packets. This is done by check-summing the packages using a cryptographic algorithm.
- ESP (Encapsulating Security Payload) that provides encryption of packets.
- IPcomp (IP payload compression) that provides compression before a packet is encrypted.
- IKE (Internet Key Exchange) provides the (optional) means to negotiate keys in secrecy.

We ARE MAKAUTIANS

ELECTRONIC MAIL SECURITY

Short Answer Type Questions

1. What is RFC 822. **[MODEL QUESTION]**

Answer:

- It is Internet email transmission protocol or SMTP.
- Supports only 7bit ASCII characters-simple text messages (English only)
- Defines format for text messages sent using e-mail
- Messages are viewed as having an envelope and content
- Envelope contains information for transmission
- Contents is the object to be delivered
- Content standard includes set of header fields used for creating envelope
- Message consists of header lines followed by unrestricted text.

2. What are the problems with normal SMTP? **[MODEL QUESTION]**

Answer:

- Do not support executable or binary files.
- Cannot transmit "Latin" like other language.
- SMTP servers may reject mail over a certain size.
- No proper mapping when ASCII translate EBCDIC
- No non-textual data handling.
- Problems in writing (deletion/addition/reordering/truncating etc.)

3. What is MIME? **[MODEL QUESTION]**

Answer:

- Stands for Multipurpose Internet Mail Extensions
- It is an extension to simple basic text messages(RFC822)
- 8-bit binary data encoding capability(both ASCII and Non-ASCII)
- can support images, sounds, movies, computer programs, multimedia.
- 5 new header fields are added such as (MIME-version, Content-Type, Content-ID, Content – Description, Content-transfer-encoding)
- Content type – seven major types and a total of fifteen subtypes
- Content transfer encoding - objective is to provide reliable delivery across the largest range of environments
- Content id – used to identify MIME entities uniquely in multiple contexts
- Content description – text description of the object with the body

4. What is the RFC for MIME? **[MODEL QUESTION]**

Answer:

MIME is specified in six linked RFC memoranda: RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289 and RFC 2049, which together define the specifications.

WE ARE MAKAUTIANS

[MODEL QUESTION]

5. What is S/MIME?

Answer:

Secure/Multipurpose Internet Mail Extension is security enhancement to MIME e-mail standard format based on technology from RSA Data Security. MIME is based on traditional e-mail format standard RFC 822.

[MODEL QUESTION]

6. What are the S/MIME Functionalities

Answer:

S/MIME has ability to sign and encrypt messages.

Enveloped data – encrypted content and encryption keys for one or more recipients

Signed data – message digest of content is encrypted using private key of sender. Content and signature are then encoded

Clear-signed data – only the digital signature is encoded.

Signed and enveloped data – signed-only and encrypted-only entities may be nested

7. What are the cryptographic algorithms used in S/MIME? [MODEL QUESTION]

Answer:

S/MIME incorporates three cryptographic algorithms

Digital Signature Standard (DSS) – for digital signature

Diffie-Hellman - for encrypting session keys (alternatives are ElGamal, RSA)

SHA-1 for creating message digest

Triple DES – for message encryption

HMAC with SHA-1 – for message authentication code

8. What is the user role in S/MIME? [MODEL QUESTION]

Answer:

Key generation, Registration and Certificate storage and retrieval.

9. What are the key requirements of message digest? [MODEL QUESTION]

Answer:

A message digest or hash function is used to turn input of arbitrary length into an output of fixed length, which is called the digest or hash of the input. This output can then be used in place of the original input. This has many advantages. The output always has the same length, so this can be taken into account when processing or storing the message digest. Also, the output is much shorter than the input, so that processing and storing can be done much quicker.

The most common cryptographic hash function is MD5. MD5 was designed by well-known cryptographer Ronald Rivest in 1991. In 2004, some serious flaws were found in MD5. The complete implications of these flaws has yet to be determined. Another popular hash function is SHA-1.

To make hash functions work, they should have two properties:

Given a particular message digest, it should be very difficult to find an input that has the same message digest.

It should be very difficult to find two inputs that have the same message digest.

WE ARE MAKAUTIANS

10. Taking $g = 11$, $n = 19$ and assuming values for A and B, find the value of K (symmetric key) by Diffie-Hellman Algorithm and prove that the algorithm is able to maintain security. **[MODEL QUESTION]**

Answer:

Here, $g = 11$, $n/p = 19$

Let choose $x = 2$, $y = 4$

$\therefore a = gx \bmod p$

$= 11^2 \bmod 19 = 7$

$b = g^y \bmod p$

$= 11^4 \bmod 19 = 11$

$\therefore k_1 = b^x \bmod p$

$= 11^2 \bmod 19 = 7$

$k_2 = a^y \bmod p$

$= 7^4 \bmod 19 = 7$

$\therefore k_1 = k_2 = k$

Long Answer Type Questions

1. Write short notes on the following:

a) PGP **[WBUT 2015]**

b) S/MIME **[MODEL QUESTION]**

Answer:

a) PGP:

PGP is a family of software systems developed by Philip R. Zimmermann.

PGP and similar products follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data. Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, E-mails, files, directories and whole disk partitions to increase the security of e-mail communications.

Open PGP provides data integrity services for messages and data files by using these core technologies:

- digital signatures
- encryption
- compression
- Radix-64 conversion

In addition, OpenPGP provides key management and certificate services.

Confidentiality via Encryption

OpenPGP combines symmetric-key encryption and public-key encryption to provide confidentiality. When made confidential, first the object is encrypted using a symmetric encryption algorithm. Each symmetric key is used only once, for a single object. A new

WE ARE MAKAUTIANS

"session key" is generated as a random number for each object (sometimes referred to as a session). Since it is used only once, the session key is bound to the message and transmitted with it. To protect the key, it is encrypted with the receiver's public key. The sequence is as follows:

1. The sender creates a message.
2. The sending OpenPGP generates a random number to be used as a session key for this message only.
3. The session key is encrypted using each recipient's public key.
   These "encrypted session keys" start the message.
4. The sending OpenPGP encrypts the message using the session key, which forms the remainder of the message. Note that the message is also usually compressed.
5. The receiving OpenPGP decrypts the session key using the recipient's private key.
6. The receiving OpenPGP decrypts the message using the session key.
   If the message was compressed, it will be decompressed.

Authentication via Digital Signature

The digital signature uses a hash code or message digest algorithm, and a public-key signature algorithm. The sequence is as follows:

1. The sender creates a message.
2. The sending software generates a hash code of the message.
3. The sending software generates a signature from the hash code using the sender's private key.
4. The binary signature is attached to the message.
5. The receiving software keeps a copy of the message signature.
6. The receiving software generates a new hash code for the received message and verifies it using the message's signature. If the verification is successful, the message is accepted as authentic.

Compression:

Open PGP implementations SHOULD compress the message after applying the signature but before encryption.

b) S/MIME:

Messages

S/MIME secures a MIME entity by signature and / or encryption

MIME entity may be entire message or one / more subparts of a message

MIME entity along with related security data are processed to produce a PKCS object which is treated as message content and wrapped in MIME. Message to be sent is converted into canonical form (i.e., a format appropriate to the content type, that is standardized for use between systems)

Resultant message (after applying security algorithm) is wrapped in an outer MIME message and transfer encoding applied.

We ARE MAKAUTIANS

Enveloped data (MIME entity)

Generate a pseudorandom session key for symmetric encryption (RC2/40 or tripleDES). Encrypt session key with recipient's public RSA key. Prepare a block RecipientInfo containing an identifier of the recipient's public-key certificate, an identifier of algorithm used to encrypt session key and encrypted session key. Encrypt the message content with the session key. Encode the entire object

Receiver's end:

Recipient first gets rid off the encoding. Recipient's private key is used to recover session key.

Finally message content is decrypted with session key.

Signed data

Select message digest algorithm (SHA or MD5). Compute message digest, or hash function, of the content to be signed. Encrypt message digest with signer's private key. Prepare a block Signer Info containing signer's public key certificate, identifier of message digest algorithm, identifier of encryption algorithm used to encrypt message digest and the encrypted message digest Signed data entity consists of a series of blocks, including a message digest algorithm identifier, message being signed and Signer Info. It may also include a set of public key certificates.

This is then encoded. Clear signing is achieved using multipart content type with a signed subtype

Registration request – the application/pkcs10 S/MIME entity is used to transfer a certification request (for public-key certificate).

Certificates-only message – message containing only certificates or a certification revocation list can be sent in response to registration request.

We ARE MAKAUTIANS

FIREWALL

Multiple Choice Type Questions

1. Firewall is a specialized form of a ..... [WBUT 2014]
   a) Bridge b) Switch c) Network d) Router

Answer: (d)

2. Application gateways are packet filters that. [MODEL QUESTION]
   a) less secure than b) more secure than
   c) equally secure to d) slower

Answer: (b)

Short Answer Type Questions

1. Discuss different types of firewall with neat diagram. [WBUT 2015]

Answer:

There are several classifications of firewalls depending on:

- Whether the communication is being done between a single node and the network, or between two or more networks.
- Whether the communication is intercepted at the network layer, or at the application layer.
- Whether the communication state is being tracked at the firewall or not.

Similarly, depending on whether the firewalls keep track of the state of network connections or treats each packet in isolation, two categories of firewalls exist:

- Stateful firewalls
- Stateless firewalls

A ***stateful firewall*** limits network information from a source to a destination based on the destination IP address, source IP address, source TCP/UDP port and destination TCP/UDP port. Stateful firewalls can also inspect date content and check for protocol anomalies. For example, a stateful firewall is much better equipped than a proxy filter or packet filter to detect and stop a denial-of-service attack. A proxy filter or paclet filter is ill-equipped and incapable of detecting such an attack. Because the source and destination address are valid, the data is permitted through whether it is legitimate or an attempted hack into the network. Figure illustrates the inspection depth of a stateful firewall. Packets are inspected upto Layer 4 of the OSI model, which is the transport layer. Therefore, stateful firewalls are able to inspect protocol anomalies.

We ARE MAKAUTIANS

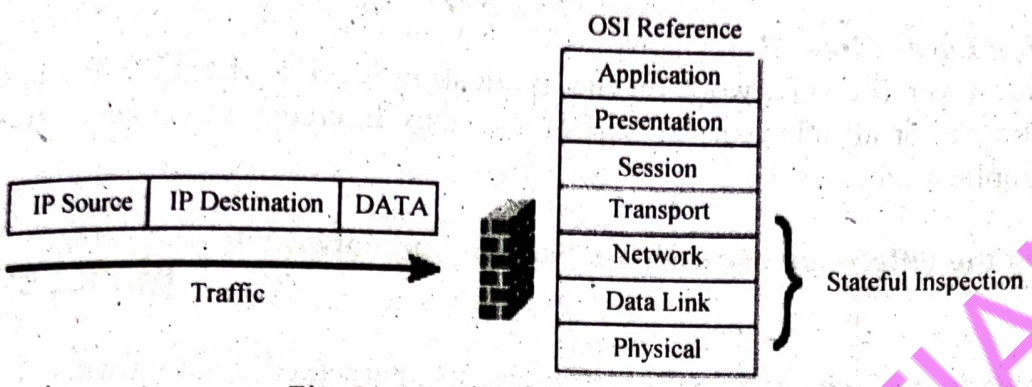


Fig: Stateful Firewall

Basically, a ***stateless firewall*** permits only the receipt of information packets that are based on the source's address and port from networks that are trusted. A stateless firewall was introduced to add more flexibility and scalability to network configuration. A stateless firewall inspects network information based on source and destination address. Figure illustrates the inspection depth of a packet filter or stateless firewall. Packets are inspected up to Layer 3 of the OSI model, which is the network layer. Therefore, stateless firewalls are able to inspect source and destination IP addresses and protocol source and destination ports.

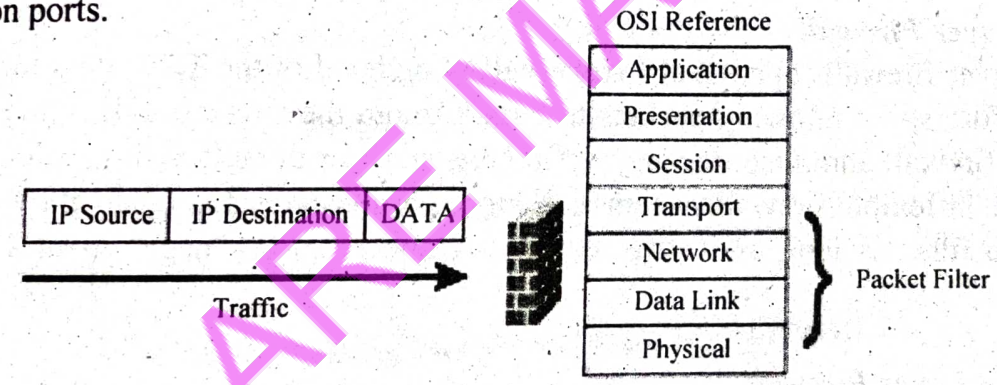


Fig: Stateless Firewall

In reference to the layers where the traffic can be intercepted, the following categories of firewalls exist:

- Network layer firewalls
- Application layer firewalls.

These network-layer and application-layer types of firewall may overlap, even though the personal firewall does not serve a network; indeed, single systems have implemented both together.

Network Layer Firewall

Network layer firewalls operate at a (relatively) low level of the TCP/IP protocol stack as IP-packet filters, not allowing packets to pass through the firewall unless they match the rules. The firewall administrator may define the rules; or default built-in rules may apply (as in some inflexible firewall systems). A more permissive setup could allow any packet to pass the filter as long as it does not match one or more "negative-rules", or "deny rules".

We ARE MAKAUTIANS

Application Layer Firewall

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application.

2. What is the difference between application and network layer firewall? **[MODEL QUESTION]**

Answer:

In reference to the layers where the traffic can be intercepted, the following categories of firewalls exist:

- Network layer firewalls
- Application layer firewalls.

These network-layer and application-layer types of firewall may overlap, even though the personal firewall does not serve a network; indeed, single systems have implemented both together.

Network Layer Firewall

Network layer firewalls operate at a (relatively) low level of the TCP/IP protocol stack as IP-packet filters, not allowing packets to pass through the firewall unless they match the rules. The firewall administrator may define the rules; or default built-in rules may apply (as in some inflexible firewall systems). A more permissive setup could allow any packet to pass the filter as long as it does not match one or more "negative-rules", or "deny rules".

Application Layer Firewall

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application.

3. What do you mean by trusted service and trusted devices in firewall configuration? **[MODEL QUESTION]**

Answer:

The list of allowed services those are specified to pass through the firewall. Examples include: WWW (HTTP), FTP, SSH, Telnet. Trusted devices allow access to your system for all traffic from that device, for example ethernet0.

WE ARE MAKAUTIANS

4. Differentiate between Packet filters and Application Gateways.

[MODEL QUESTION]

Answer:

Packet Filters

In packet filters some rules are stored previously and whenever any packet comes from outside it applies those set of rules to incoming packet and on basis of rules it decides whether give permission for go inside or discard the packet. They also apply same action if packets are going outside from inside. Packet filters are also known as screening filter or screening router. Now you might be thinking that on which basis set of rules are defined. So let me tell you that set of rules are defined on basis of number of fields in internet protocol and tcp(transmission control protocol) or udp(user datagram protocol) header. Packet filters are extremely fast during their operating speed. In this way packet filters are providing protection to the local system or private networks from outside network. But there is one disadvantage is that setting up rules is too difficult.

Application Gateway

Application gateway is one type of firewall which protects local system or private networks from outside network. It is also known as proxy server because it behaves like any proxy server and decides the flow of application.

Circuit gateway is variation of application gateway. It establishes a new connection between remote host and itself. User is not aware about this connection and he/she thinks that he/she is directly connected to the remote host. Circuit gateway changes the ip address of end user and because of that source ip address are stay hidden from outside network. As per my opinion Application gateways are more secure then packet filters.

Long Answer Type Questions

1. What is firewall? What are the different types of firewall? State the limitations of firewall.

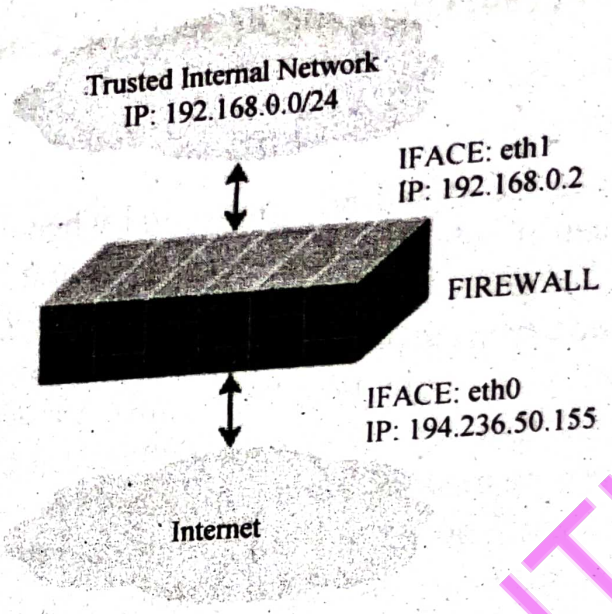
[WBUT 2014]

Answer:

1st Part:

A firewall blocks traffic to all except authorized ports on a computer, thus restricting access. A stateful firewall is even more cautious about what it permits through, and the most cautious system administrators often combine a proxy firewall with a packet-filtering firewall to create defense in depth. Most home users would use a software firewall, while some high risk servers and computers might need a hardware firewall. By inspecting all packets for improper content, firewalls can even prevent the spread of the likes of viruses.

We ARE MAKAUTIANS



2nd Part: ***Refer to Question No. 1 of Short Answer Type Questions.***

3rd Part:

A firewall cannot protect against:

- malicious insiders
- connections that circumvent it
- completely new threats
- some viruses
- the administrator that does not correctly set it up

2. Write short notes on the following: **[MODEL QUESTION]**

a) Application firewalls

b) DMZ

c) Packet filtering

Answer:

a) Application firewalls:

Application-layer firewalls are aware of certain applications, such as the Web, SQL, and e-mail. Also, these multi-talented firewalls prohibit direct connections from the Internet to your servers by acting as a proxy between the applications you serve (Web, E-mail, FTP, etc.) to the rest of the wired world.

An application-level firewalls' excellence is in going deep into a packet's application payload on a session level. Deciding before your sever receives each packet, whether the data portion of the packet is a normal part of a TCP/IP conversation, or malformed and part of a virus or a known exploit.

An application-layer filter is essential when it comes to Web, e-mail, and SQL servers, which are high profile targets for application exploits. The firewall makes decisions at the application level before the server sees the malformed command. It inspects and passes normal SMTP commands but stops spammers cold when they try to verify and enumerate your e-mail .In addition, Web application filtering on some of the best application-layer

We ARE MAKAUTIANS

devices (Firewall 1NG-Check Point, Symantec Enterprise Firewall – Symantec and ISA – Microsoft) easily blocks the latest URL string patterns and Unicode expressions, which is a nice defense against those nasty directory traversal attacks that seem to pop up every other month.

These generally are hosts running proxy servers, which permit no traffic directly between networks, and which perform elaborate logging and auditing of traffic passing through them. Since the proxy applications are software components running on the firewall, it is a good place to do lots of logging and access control. Application layer firewalls can be used as network address translators, since traffic goes in one side and out the other, after having passed through an application that effectively masks the origin of the initiating connection. Having an application in the way in some cases may impact performance and may make the firewall less transparent. Early application layer firewalls such as those built using the TIS firewall toolkit, are not particularly transparent to end users and may require some training. Modern application layer firewalls are often fully transparent. Application layer firewalls tend to provide more detailed audit reports and tend to enforce more conservative security models than network layer firewalls.

b) DMZ:

Hosts in the DMZ are permitted to have only limited connectivity to specific hosts in the internal network, as the content of DMZ is not as secure as the internal network. Similarly communication between hosts in the DMZ and to the external network is also restricted, to make the DMZ more secure than the Internet, and suitable for housing these special purpose services. This allows hosts in the DMZ to communicate with both the internal and external network. There are two basic configuration exists for a DMZ : single firewall or three legged model and dual firewall .

In a three legged model the external network is formed from the ISP to the firewall on the first network interface, the internal network is formed from the second network interface, and the DMZ is formed from the third network interface. The firewall becomes a single point of failure for the network and must be able to handle all of the traffic going to the DMZ as well as the internal network.

In dual firewall approach two firewalls are used to create a DMZ. The first firewall or front-end or perimeter firewall must be configured to allow traffic destined to the DMZ only. The second firewall (also called "back-end" or "internal" firewall) only allows traffic from the DMZ to the internal network.

c) Packet filtering:

A packet filter is a set of rules defining the security policy of a network. In practice, these rules are based on the values of fields in the IP or transport layer headers. Any field of the IP or transport header can be used in a firewall rule, but the most common ones are:

- filter on the source address. For example, a company may decide to discard all packets received from one of its competitors. In this case, all packets whose source address belong to the competitor's address block would be rejected

WE ARE MAKAUTIANS

- filter on destination address. For example, the hosts of the research lab of a company may receive packets from the global Internet, but not the hosts of the financial department
- filter on the *Protocol* number found in the IP header. For example, a company may only allow its hosts to use TCP or UDP, but not other, more experimental, transport protocols
- filter on the TCP or UDP port numbers. For example, only the DNS server of a company should be received UDP segments whose destination port is set to *53* or only the official SMTP servers of the company can send TCP segments whose source ports are set to *25*

A simple router is the traditional network layer firewall, since it is not able to make particularly sophisticated decisions about what a packet is actually talking to or where it actually came from. Modern network layer firewalls have become increasingly sophisticated, and now maintain internal information about the state of connections passing through them, the contents of some of the data streams, and so on. Network layer firewalls tend to be very fast and tend to be very transparent to users.

We ARE MAKAUTIANS