UNIT 5

What is cryptography?

2.1

1. What is cryptography? What is it used for?

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.
It's used for diplomatic, during war, individual or corporate privacy.

2. Where does cryptography derive from and what does it mean?

The word “cryptography” is derived from the Greek words kryptos, meaning hidden, and graphien, meaning to write.

3. What aspects of information security does cryptography relate?

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

4. What is cryptanalysis?

Cryptanalysis or crypto-analysis is the study and analysis of existing ciphers or encryption algorithms, (or Cryptanalysis is the process of obtaining the original message (called the plaintext) from an encrypted message (called the ciphertext) without knowing the algorithms and keys used to perform the encryption) in order to assess their quality, to find weaknesses or to find a way to reverse the encryption process without having the key.

5. What is encryption? What is decryption?

The process of making the information unreadable is called encryption or enciphering. The result of encryption is a ciphertext or cryptogram.
Reversing this process and retrieving the original readable information is called decryption or deciphering.

6. Why does cryptanalysis study and analyze existing ciphers or encryption algorithms?

Because they are used to assess their quality, to find weaknesses or to find a way to reverse the encryption process without having the key.

7. How many goals does cryptography have? What are they?

There are four cryptographic goals:
Confidentiality is a service used to keep the content of information from all but those authorized to have it.
Data integrity is a service which addresses the unauthorized alteration of data.
Authentication is a service related to identification.
Non-repudiation is a service which prevents an entity from denying previous commitments or actions.

8. What major classes of authentication usually subdivided? Why is it subdivided so?

Authentication is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc so major classes of authentication usually subdivided : entity authentication and data origin authentication.

2.3

1. Which process needs the key?
encryption and decryption

2. What types of attacks are mentioned in the text?
Brute force attack, Ciphertext-only attack, Known - plaintext attack
3. A .....is to adequately address confidentiality, data integrity, authentication, and non-repudiation in both theory and practice.
fundamental goal of cryptography
4. ……is a service which prevents an entity from denying previous commitments or actions.
Non-repudiation
5. What was considered an early instance of encipherment?
Egyptian hieroglyphics
6. A service related to verification. This function is for both parties and information itself is …….....
authentication
7. Which of the following attacks that can, in theory, be used to attempt to decrypt any encrypted data?
A brute-force attack
8. Which of the followings is the study of analyzing information systems in order to study the hidden aspects of the systems?
Cryptanalysis

Foundations of Cryptography

2.1

1. When was cryptography changed from dark art into a science based on mathematics? Who changed it?
Auguste Kerckhoff was one of the most important men changed cryptography from dark art into a science based on mathematics in the end of the 19th century.
2. Who was the father of Information Theory?
Claude Elwood Shannon was the father of Information Theory.
3. What device was developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication?
The Enigma machine was developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication.
4. Who invented Enigma machine and when was it invented?
Arthur Scherbius invented Enigma machine in 1927
5. Who introduced the idea of public-key cryptography? What are its algorithms based on? the computational complexity problem.
Whitefield Diffie and Martin Hellman introduced the idea of public-key cryptography of which algorithms are based on the computational complexity problem. The Diffie–Hellman algorithms are based on the discrete logarithm problem.
6. What device was developed by the Spartans of Greece? When was it developed?
The Spartans of Greece developed the scytale, a system consisting of a strip of papyrus wrapped

around a wooden staff in 487 B.C
7. What did Leon Battista Alberti invented?
Leon Battista Alberti invented a device based on two concentric discs that simplified the use of Caesar ciphers

8. Which algorithms are the most widely used in the world among crypto algorithms?

the Diffie–Hellman algorithms and RSA are among the most widely used crypto algorithms in the world.

2.3

1. Who invented one-time pad encryption for Telex Traffic
Gilbert S. Vernam
2. What cipher did Julius Caesar use to secure military and government communications?
Monoalphabetic substitution cipher and simple substitution cipher
3. What is one of the most significant contribution provided by public-key cryptography?
the digital signature
4. When was the Enigma cipher broken? Who broke it?
In1939 -1942/The Allies
5. Which of the followings is one of the first block ciphers?
Lucifer cipher
6. Who broke Japan's Purple's ciphers?
William Friedman
7. What types of cipher were used in radio communications during World War I?
Transposition ciphers and Substitution ciphers
8. Why did the United States decide to take part in World War II?
Because the Enigma machine was broken.

Some basic terminology and concepts

2.1

1. What do the letter A,M,C,K denote?
A denotes a finite set called the alphabet of definition.
M denotes a set called the message space. M consists of strings of symbols from an alphabet of definition.
C denotes a set called the ciphertext space. C consists of strings of symbols from an alphabet of definition, which may differ from the alphabet of definition for M. An element of C is called a ciphertext.
K denotes a set called the key space. An element of K is called a key.
2. Which letters denote a key pair?
e and d denote a key pair
3. What is Dd called?
Dd is called a decryption function or decryption transformation.

4. What does an encryption scheme consist of?

- An *encryption scheme* consists of a set $\{E_e : e \in K\}$ of encryption transformations and a corresponding set $\{D_d : d \in K\}$ of decryption transformations with the property that for each e K there is a unique key $d \in K$ such that $D_d = E_2^{-1}$; that is, $D_d (E_e (m)) = m$ for all $m \in M$. An encryption scheme is sometimes referred to as *a cipher*.

5. What does one have to do to construct an encryption scheme?
To construct an encryption scheme requires one to select a message space M, a ciphertext space C, a key space K, a set of encryption transformations {Ee : e ∈ K} and a corresponding set of decryption transformations {Dd : d ∈ K} .
6. What does the owner of the key do if he suspects that the combination has been revealed?
If the owner suspects that the combination has been revealed he can easily reset it without replacing the physical mechanism.
7. How is an encryption scheme used to achieve confidentiality?
An encryption scheme may be used as follows for the purpose of achieving confidentiality. Two parties Alice and Bob first secretly choose or secretly exchange a key pair (e, d). At a subsequent point in time, if Alice wishes to send a message m ∈ (belong to) M to Bob, she computes c = Ee (m) and transmits this to Bob. Upon receiving c, Bob computes Dd (c) = m and hence recovers the original message m.

2.3
1. An element of M is called …….....
a plaintext message or simply a plaintext
2. An element of K is called …….....
a key
3. An element of C is called …….....
a ciphertext
4. One has to …… if some particular encryption or decryption transformation is revealed.
change the key
5. The structure of the lock ……but the combination is chosen and set by the owner.
is available to anyone who wants to purchase one
6. The diagram in Figure 5-3. Schematic of a simple encryption scheme is good for describing an encryption scheme…….
When is a small set

Communication participants

2.1
1. What is the difference among a sender, a receiver, and an adversary?

A sender is an entity in a two-party communication which is the legitimate transmitter of information.
A receiver is an entity in a two-party communication which is the intended recipient of information.
An adversary is an entity in a two-party communication which is neither the sender nor receiver, and which tries to defeat the information security service being provided between the sender and receiver.
2. What are unsecured channel and secured channel?
An unsecured channel is one from which parties other than those for which the information is intended can reorder, delete, insert, or read.
A secured channel is one from which an adversary does not have the ability to reorder, delete, insert, or read.
3. What is the only thing that the two parties keep secret when using an encryption scheme?
When two parties wish to communicate securely using an encryption scheme, the only thing that they keep secret is the particular key pair (e, d) which they are using, and which they must select.

4. Can an encryption scheme be broken? When and how?
An encryption scheme can be broken if a third party, without prior knowledge of the key pair (e, d), by trying all possible keys to see which one the communicating parties are using.
5. What is called an exhaustive search?
An encryption scheme can be broken by trying all possible keys to see which one the communicating parties are using (assuming that the class of encryption functions is public knowledge). This is called an exhaustive search of the key space.
6. What is the objective of a designer of an encryption scheme?
the objective of a designer of an encryption scheme is the best approach to break the system.
7. What did Kerckhoff articulate in 1883 in his famous literature?
chịu, tìm lòi mắt k có trong bài :v
8. What is the difference between an active adversary and a passive adversary?
An active adversary is an adversary who may also transmit, alter, or delete information on an unsecured channel.
A passive adversary is an adversary who is capable only of reading information from an unsecured channel.
2.3
1. Which channel is not physically accessible to the adversary?
A physically secure channel or secured channel
2.Which role does an adversary attempt to play in a two-way communication?
the legitimate sender or the legitimate receiver
3. What is a fundamental premise in cryptography?
the sets M, C, K {Ee : e K}, {Dd : d K}
4. A/An ……is an entity in a two-party communication which is the legitimate transmitter of information.
sender
5. A/An …… is an entity in a two-party communication which is the intended recipient

of information.
receiver
6.…….. an information security service implies defeating the objective of the intended service.
Breaking
7. A/An ……is an adversary who is capable only of reading information from an unsecured channel.
passive adversary
8. A/An ….. is a means of conveying information from one entity to another.
channel
9. An ……is an adversary who may also transmit, alter, or delete information on an unsecured channel.
active adversary
10.……is a method to provide some specific aspects of security.
Information security service

UNIT 6

Hash functions

2.1

1. What are Hash functions?
Hash functions are mathematical algorithms that generate a message summary or digest (sometimes called a fingerprint) to confirm the identity of a specific message and to confirm that there have not been any changes to the content.
2. Why are hash functions considered one-way operations?
Because in that the same message always provides the same hash value, but the hash value itself cannot be used to determine the contents of the message.
3. What is the message digest?
The message digest is a fingerprint of the author's message that is compared with the recipient's locally calculated hash of the same message.
4. Why are hash functions widely used in e-commerce?
Because while they do not create a ciphertext, hash functions confirm message identity and integrity, both of which are critical functions in e-commerce.
5. What does SHS stand for? What is it?
The Secure Hash Standard (SHS) is a standard issued by the National Institute of Standards and Technology (NIST).
6. What are hash algorithms?
Hash algorithms are public functions that create a hash value, also known as a message digest, by converting variable-length messages into a single fixed-length value.
7. What is a measurement of the strength of the algorithm against collision attacks?
The number of bits used in the hash algorithm is a measurement of the strength of the algorithm against collision attacks.

8. What attack method has become a concern about the strength of the processes used for password hashing?
A recent attack method called rainbow cracking has generated concern about the strength of the processes used for password hashing.

2.3

1. Why are hash functions used in password verification systems to confirm the identity of the user?
Because hash functions are one-way.
2. What will attackers do if they gain access to a file of hashed passwords?
They can use a combination of brute force and They can use dictionary attacks to reveal user passwords
3. What do users have to do to prevent rainbow cracking?
They have to protect the file of hashed passwords
They have to implement strict limits to the number of attempts allowed per login session
They have to use an password hash salting approach
4. Which passwords are considered easily to be cracked?
Passwords that are dictionary words or poorly constructed
5. .....is the process of providing a non-secret, random piece of data to the hashing function when the hash is first calculated.
Salting

6. What specifies SHA-1 as a secure algorithm for computing a condensed representation of a message or data file?
Standard document FIPS 180-1
7. Which applications in the information security do cryptographic hash functions bring?
digital signatures, message authentication codes (MACs), and other forms of authentication
8. Which of the following properties that an ideal cryptographic hash function needs to have?
It is easy to compute the hash value for any given message
It is infeasible to generate a message that has a given hash
It is infeasible to modify a message without changing the hash
It is infeasible to find two different messages with the same hash

Symmetric Encryption

2.1

1. What is the primary challenge of symmetric key encryption?
The primary challenge of symmetric key encryption is getting the key to the receiver, a process that must be conducted out of band (meaning through a channel or band other than the one carrying the ciphertext) to avoid interception.
2. What symmetric encryption cryptosystems is one of the most widely known?
One of the most widely known is the Data Encryption Standard (DES)
3. What is called symmetric encryption?

Encryption methodologies that require the same secret key to encipher and decipher the message are using what is called private key encryption or symmetric encryption.
4. When was a DES key broken and who broke it?
In 1998, a group called the Electronic Frontier Foundation (www.eff.org), using a specially designed computer, broke a DES key in less than three days.
5. Why do symmetric encryption methods use mathematical operations that can be programmed into extremely fast computing algorithms?
Symmetric encryption methods use mathematical operations that can be programmed into extremely fast computing algorithms so that the encryption and decryption processes are executed quickly by even small computers.
6. What are the disadvantages of symmetric encryption method?
One of the challenges is that both the sender and the recipient must have the secret key. Also, if either copy of the key falls into the wrong hands, messages can be decrypted by others and the sender and intended receiver may not know the message was intercepted.
7. Why was Advanced Encryption Standard born?
Because AES has been developed to replace both DES and 3DES.
8. What is the difference between DES and AES?
DES uses a 64-bit block size and a 56-bit key.
AES implements a block cipher called the Rijndael Block Cipher with a variable block length and a key length of 128, 192, or 256 bits.

2.3
1. What is Data Encryption Standard based on?
Lucifer algorithm
2. The requirements for AES stipulate that the algorithm should .....
be unclassified
be publicly disclosed
available royalty-free worldwide
3. When was Data Encryption Standard found unsafe?
In 1997
4. Which of the following agencies in the U.S are allowed to use AES to protect information?
Agencies that are not a part of the national defense infrastructure.
5. Which of the followings has the highest level of security?
AES

Asymmetric Encryption

2.1
1. What is asymmetric encryption?
Asymmetric encryption uses two different but related keys, and either key can be used to encrypt or decrypt the message. If, however, key A is used to encrypt the message, only key B can decrypt it, and if key B is used to encrypt a message, only key A can decrypt it.
2. What asymmetric encryption cryptosystems is one of the most popular public key

cryptosystems?
One of the most popular public key cryptosystems is RSA
3. What is the foundation of public-key encryption?
Asymmetric algorithms are one-way functions. A one-way function is simple to compute in one direction, but complex to compute in the opposite direction. This is the foundation of public-key encryption.
4. What is the highest value of the asymmetric encryption when one key is used as a private key?
The highest value of the asymmetric encryption when one key is used as a private key is kept secret (much like the key in symmetric encryption), known only to the owner of the key pair, and the other key serves as a public key, which means that it is stored in a public location where anyone can use it.
5. What is a mathematical trapdoor?
A mathematical trapdoor is a “secret mechanism that enables you to easily accomplish the reverse function in a one-way function.”.
6. What is public-key encryption based?
Public-key encryption is based on a hash value, which is calculated from an input number using a hashing algorithm. This hash value is essentially a summary of the original input values. It is virtually impossible to derive the original values without knowing how those values were used to create the hash value.
7. What can users do and what can’t they do with a trapdoor?
With a trapdoor, you can use a key to encrypt or decrypt the ciphertext, but not both, thus requiring two keys. The public key becomes the true key, and the private key is derived from the public key using the trapdoor.

2.3
1. Who developed RSA algorithm?
Ron Rivest, Adi Shamir, Leonard Adleman
2. What is the disadvantage of RSA?
Holding a single conversation between two parties requires four keys.
3. What must four organizations do if they want to communicate?
Each party must manage its private key and four public keys.
4. In which of the following uses is RSA useful?
Commercial use
5. Where is RSA embedded?
In Microsoft and Netscape Web browsers

Public-key Infrastructure

2.1
1. What does PKI stand for? What is it?
Public-key Infrastructure (PKI) is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely.
2. What components are integrated for a typical solution PKI to protect the transmission and

reception of secure information?
A typical PKI solution protects the transmission and reception of secure information by integrating the following components:

- A certificate authority (CA), which issues, manages, authenticates, signs, and revokes users' digital certificates, which typically contain the user name, public key, and other identifying information.
- A registration authority (RA), which operates under the trusted collaboration of the certificate authority and can handle day-to-day certification functions, such as verifying registration information, generating end-user keys, revoking certificates, and validating user certificates.
- Certificate directories, which are central locations for certificate storage that provide a single access point for administration and distribution.
- Management protocols, which organize and manage the communications among CAs, RAs, and end users. This includes the functions and procedures for setting up new users, issuing keys, recovering keys, updating keys, revoking keys, and enabling the transfer of certificates and status information among the parties involved in the PKI's area of authority.
- Policies and procedures, which assist an organization in the application and management of certificates, in the formalization of legal liabilities and limitations, and in actual business use.

3. What do common implementations of PKI include?
Common implementations of PKI include systems that issue digital certificates to users and servers; directory enrollment; key issuing systems; tools for managing the key issuance; and verification and return of certificates.
4. What does the strength of a cryptosystem rely?
The strength of a cryptosystem relies on both the raw strength of its key's complexity and the overall quality of its key management security processes.

5. What are digital certificates?
Digital certificates are public-key container files that allow computer programs to validate the key and identify to whom it belongs.
6. What is critical to the successful use of encryption and nonrepudiation services within the PKI's area of trust.10?
Managing the security and integrity of the private keys used for nonrepudiation or the encryption of data files is critical to the successful use of encryption and nonrepudiation services within the PKI's area of trust.10
7. What are Public-key Infrastructure systems based on?
PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs).
8. What mechanisms can PKI solutions provide for limiting access and possible exposure of the private keys?
These mechanisms include password protection, smart cards, hardware tokens, and other hardware-based key storage devices that are memory-capable (like flash memory or PC memory cards).

2.3

1. What can the CA do when the user loses the privilege of using keys in the area of authority?

The CA can withdraw the user's keys.
The CA can revoke the user's keys.
2. What is the function of a central system operated by a CA?
It generates cryptographically strong keys that are considered by all users to be independently trustworthy.
It provides private key backup, key recovery, and key revocation.
3. Which mechanisms should PKI users select in digital certification?
The key security mechanisms that provide a level of key protection appropriate to their needs.
4. The .....by the CA enables secure, encrypted, nonrepudiable e-business transactions.
mechanisms of certificate
5. How often does the CA distribute a certificate revocation list to all users?
Regulary

Attacks on Cryptosystems

2.1

1. What are correlation attacks?
Correlation attacks are a collection of brute-force methods that attempt to deduce statistical relationships between the structure of the unknown key and the ciphertext generated by the cryptosystem.
2. What method can prevent correlation attacks?
The only defense against this attack is the selection of strong cryptosystems that have stood the test of time, thorough key management, and strict adherence to the best practices of cryptography in the frequency of key changes.

3. What is a man-in-the-middle attack?
A man-in-the-middle attack attempts to intercept a public key or even to insert a known key structure in place of the requested public key.
4. What method can prevent the traditional man in-the-middle attack?
Establishing public keys with digital signatures can prevent the traditional man in-the-middle attack, as the attacker cannot duplicate the signatures.
5. When can dictionary attacks be successful?
Dictionary attacks can be successful when the ciphertext consists of relatively few characters, as for example files which contain encrypted usernames and passwords.
6. When may the attacker launch a replay attack in timing attack?
Having broken an encryption, the attacker may launch a replay attack, which is an attempt to resubmit a recording of the deciphered authentication to gain entry into a secure source.
7. What method was used to get unauthorized access to secure communications?
to get unauthorized access to secure communications have used brute force attacks
8. What type of attacks are mentioned according to the text?
brute force attacks, known-plaintext attack, selected-plaintext attack, Man-in-the-Middle Attack,

Correlation Attacks, Dictionary Attacks, Timing Attacks

2.3

1. What attacks were used to gain unauthorized access to secure communications?

Brute force attacks

known-plaintext attacks

selected –plaintex attacks

2. Attackers may conduct a .....by sending potential victims a specific text that they are sure the victims will forward on to others.

selected-plaintext attack

3. .....have been used to mount successful attacks on block cipher encryptions such as DES.

Differential and linear cryptanalysis

4. In which attack does the attacker eavesdrop on the victim's session?

In a timing attack

5. Which of the following does the word "these" in the paragraph 6 refer to?

Differential and linear cryptanalysis