Information Security

Chapter 3:

3.1 What are the two principal requirements for the secure use of symmetric encryption?
(1) a strong encryption algorithm;
(2) Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

3.2 What are the two basic functions used in encryption algorithms?
Substitution and transposition are the two basic functions used in encryption algorithms.

3.3 Differentiate between secret-key encryption and public-key encryption
n this, the same key (secret key) and algorithm are used **to encrypt and decrypt the message**. In public-key cryptography, two keys are used, one key is used for encryption

and while the other is used for decryption. Private key is Symmetrical because there is only one key that is called a secret key.

3.4 What is the difference between a block cipher and a stream cipher?
A **block cipher processes the input one block of elements at a time**, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

3.5 What are the two general approaches to attacking a cipher?

There are two general approaches to attacking a conventional encryption scheme:
Cryptanalysis (cryptanalytic attacks): This attack relies on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext or some sample plaintext–ciphertext pairs. It exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

3.6 List and briefly define types of cryptanalytic attacks based on what is known to the attacker.

Types of Cryptanalytic attacks:

- **Known-Plaintext Analysis (KPA) :**
  In this type of attack, some plaintext-ciphertext pairs are already known. Attackers map them in order to find the encryption key. This attack is easier to use as a lot of information is already available.
- **Chosen-Plaintext Analysis (CPA) :**
  In this type of attack, the attacker chooses random plaintexts and obtains the corresponding ciphertexts, and tries to find the encryption key. It's very simple to implement like KPA but the success rate is quite low.
- **Ciphertext-Only Analysis (COA) :**
  In this type of attack, only some cipher-text is known and the attacker

tries to find the corresponding encryption key and plaintext. It is the hardest to implement but is the most probable attack as only ciphertext is required.

- **Man-In-The-Middle (MITM) attack :**
  In this type of attack, an attacker intercepts the message/key between two communicating parties through a secured channel.
- **Adaptive Chosen-Plaintext Analysis (ACPA) :**
  This attack is similar to CPA. Here, the attacker requests the ciphertexts of additional plaintexts after they have ciphertexts for some texts

3.7 What is the difference between an unconditionally secure cipher and a computationally secure cipher?

An encryption scheme is unconditionally secure **if the ciphertext generated by the scheme does not contain enough information to uniquely determine the corresponding plaintext**, no matter how much ciphertext is available.

Unconditionally secure = no amount of computer power can recover the plain text given the ciphertext.

Computationally secure = The encryption algorithm has been proven through mathematical analysis to resist any “shortcuts” which allow recovery of plain text from the ciphertext.

3.8 Why is the Caesar cipher substitution technique vulnerable to brute-force cryptanalysis?

Because **there are only 25 possible keys**, Caesar ciphers are very vulnerable to a “brute force” attack, where the decoder simply tries each possible combination of letters. For example, the letter E appears more often than any other one whereas Z appears the least often.

3.9 How much keyspace is available when a monoalphabetic substitution cipher is used to replace plaintext with ciphertext?

The cipher has a keyspace of a cryptographic algorithm whose key length is n is given by 2^n, but the keyspace of the substitution cipher is 2^88 which is an approximation of 26!. (Considering an alphabet of 26 letters)

3.10 What is the drawback of a Playfair cipher?

The main drawback of the traditional Playfair cipher is that **the plain text can consist of 25 uppercase letters only**. One letter has to be omitted and cannot be reconstructed after decryption. Also, lowercase letters, white space, numbers, and other printable characters cannot be handled by the traditional cipher.

3.11 What is the difference between a monoalphabetic cipher and a polyalphabetic cipher?

1. Monoalphabetic Cipher: A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to ciphertext letters based on a single alphabetic key. Examples of monoalphabetic ciphers would include the Caesar-shift cipher, where each letter is shifted based on a numeric key, and the atbash cipher, where each letter is mapped to the letter symmetric to it about the center of the alphabet.

2. Polyalphabetic Cipher: A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

3.12 What are two problems with the one-time pad?

The main disadvantage of encryption with the one-time pad is that **it requires a pad of the same length as the message to be encrypted**. Since each pad can only be used

once, this means that it is necessary to share a pad of the same length as the message to be shared.

3.13 What is a transposition cipher?

Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a ciphertext. In this process, the actual plain text alphabets are not included.

Example

A simple example for a transposition cipher is a columnar transposition cipher where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different ciphertext.

Consider the plain text hello world, and let us apply the simple columnar transposition technique as shown below

h	e	l	l
o	w	o	r
l	d		

The plain text characters are placed horizontally and the ciphertext is created with a vertical format as holed LR. Now, the receiver has to use the same table to decrypt the ciphertext to plain text.

3.14 What are the drawbacks of Steganography?

One of steganography's disadvantages is that **there is a large overhead to hide very tiny amounts of information**. Hiding short messages within the wide text is limited by the size of the extensive text. Text files cleanly aren't big enough to cover more complex data like images or audio files.

Chapter 4:

4.1 Briefly define a nonsingular transformation.

Nonsingular Transformation: Nonsingular Transformation means **the encryption algorithm must be reversible (Nonsingular) to decrypt the ciphertext into the original plaintext**. The ciphertext must be unique for each plaintext block.

4.2 What is the difference between a block cipher and a stream cipher?

A block cipher **breaks down plaintext messages into fixed-size blocks** before converting them into ciphertext using a key. Encrypting information bit-by-bit. A stream cipher, on the other hand, breaks a plaintext message down into single bits, which then are converted individually into ciphertext using key bits.

4.3 Why is it not practical to use an arbitrary reversible substitution cipher of the kind shown in Table 4.1?

Table 4.1:Encryption and Decryption Tables for Substitution Cipher of Figure 4.2 in the tosecurelyubstitution and permutation of the term with textbook.

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Ciphertext	Plaintext

0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

4.4 Briefly define the substitution and permutation of the terms.

Substitution replaces plaintext letters or strings of letters with letters or numbers or symbols. Permutation uses the plaintext message letters but rearranges their order.

4.5 What is the difference between diffusion and confusion?

The terms confusion and diffusion are the properties for making a secure cipher. Both Confusion and diffusion are used to prevent the encryption key from its deduction or ultimately for preventing the original message. Confusion is used for creating clueless ciphertext while diffusion is used for increasing the redundancy of the plaintext over the major part of the ciphertext to make it obscure. The stream cipher only relies on confusion. Alternatively, diffusion is used by both stream and block cipher.

Comparison Chart

BASIS FOR COMPARISON	CONFUSION	DIFFUSION
Basic	Utilized to generate vague ciphertexts.	Utilized to generate obscure, plain texts.
Seeks to	Make a relation between the statistics of the ciphertext and the value of the encryption key as complicated as possible.	The statistical relationship between the plaintext and ciphertext is made as complicated as possible.
Achieved through	Substitution algorithm	Transposition algorithm
Used by	Block cipher only.	Stream cipher and block cipher
Result in	Increased vagueness	Increased redundancy

4.6 Which parameters and design choices determine the actual algorithm of a Feistel cipher?

Feistel cipher may have **invertible, non-invertible, and self invertible components** in its design. Same encryption, as well as decryption algorithm, is used. A separate key is used for each round. However, the same round keys are used for encryption as well as decryption.

4.7 What are the critical aspects of Feistel cipher design?

Feistel Cipher model is a structure or a design used to develop many block ciphers such as DES. Feistel cipher may have invertible, non-invertible, and self invertible components in its design. Same encryption, as well as decryption algorithm, is used. A separate key is used for each round. However, the same round keys are used for encryption as well as decryption.

Feistel cipher algorithm

- Create a list of all the Plain Text characters.
- Convert the Plain Text to Ascii and then 8-bit binary format.
- Divide the binary Plain Text string into two halves: left half (L1)and right half (R1)
- Generate random binary keys (K1 and K2) of length equal to half the length of the Plain Text for the two rounds.

Chapter 9:

9.1 What is a public key certificate?

A public-key certificate is **a digitally signed document that serves to validate the sender's authorization and name**. It uses a cryptographic structure that binds a public key to an entity, such as a user or organization.

9.2 What are the roles of the public and private keys?

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

9.3 What are three broad categories of applications of public-key cryptosystems?

Encryption/decryption: The sender encrypts a message with the recipient's public key.

Digital signature: The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

Key exchange: Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

9.4 What requirements must a public-key cryptosystem fulfill to be a secure algorithm?

1. It is computationally easy for party B to generate a pair
(public key PUb , private key PRb).

2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M , to generate the corresponding ciphertext: C = E(PUb , M)

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message:
M = D(PRb , C) = D(PRb , E(PUb , M))

4. It is computationally infeasible for an opponent, knowing the public key, PUb , to determine the private key, PRb .

5. It is computationally infeasible for an opponent, knowing the public key, PUb , and a ciphertext, C , to recover the original message, M

9.5 How can a probable-message attack be used for public-key cryptanalysis?

Using the public key algorithms, a message encrypted with one key can be decrypted only with the other. The two possible keys give us two possible ways of sending messages. **Encrypt with the private key**, decrypt with the public, or encrypt with the public key, decrypt with the private.

9.6 List the different approaches to attack the RSA algorithm.
Below is the list of some possible attacks on RSA algorithm:

- Plaintext Attack. Plain text attacks are classified into three categories.
- Chosen cipher Attack. In this type of attack, the attacker can find out the plain text from ciphertextpublic-keypublic-keypublic-key using the extended euclidean algorithm.
- Factorization Attack.

9.7 Describe the countermeasures to be used against the timing attack.

Two types of countermeasures can be applied against timing attacks. **The first one consists in eliminating timing variations whereas the second renders these variations useless for an attacker**. The only absolute way to prevent timing attacks is to make the computation strictly constant time, independent of the input.

Chapter 10:

10.1 Briefly explain Diffie–Hellman key exchange.

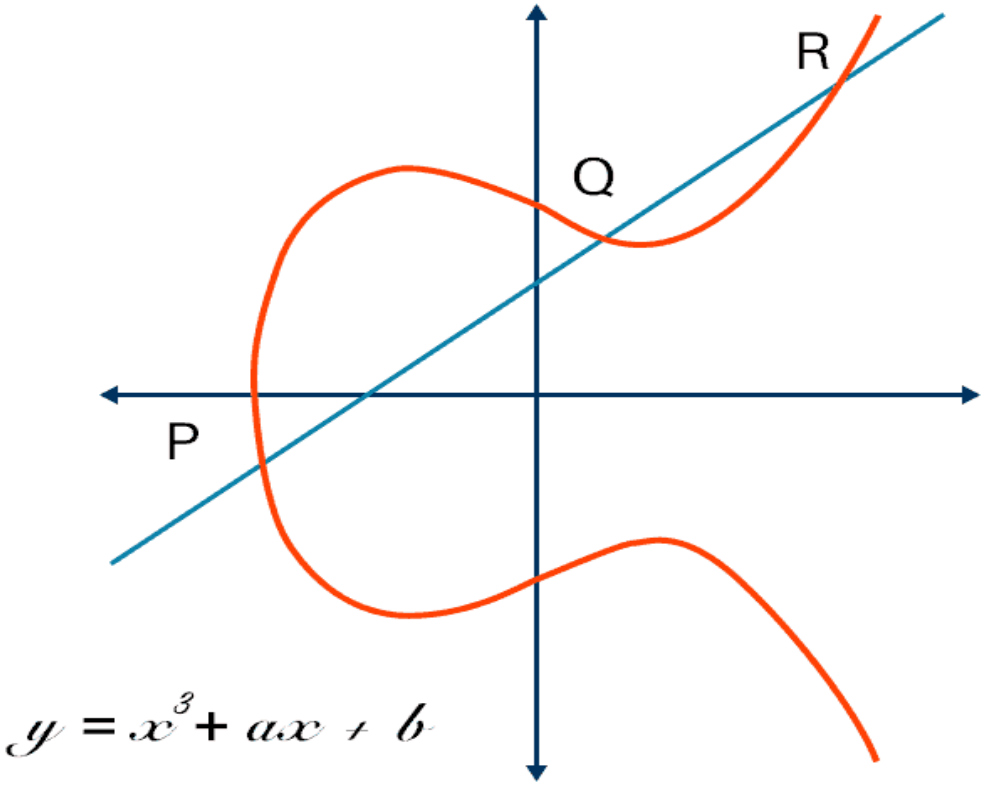
The Diffie–Hellman (DH) Algorithm is a **key-exchange protocol that enables two parties communicating over a public channel to establish a mutual secret without it being transmitted over the Internet**. DH enables the two to use a public key to encrypt and decrypt their conversation or data using symmetric cryptography.

10.2 What is an elliptic curve?

Elliptic Curve Cryptography Definition

Elliptic Curve Cryptography (ECC) is a key-based technique for encrypting data. ECC focuses on pairs of public and private keys for decryption and encryption of web traffic.

ECC is frequently discussed in the context of the Rivest–Shamir–Adleman (RSA) cryptographic algorithm. RSA achieves one-way encryption of things like emails, data, and software using prime factorization.



ECC, an alternative technique to RSA, is a powerful cryptography approach. It generates security between key pairs for public key encryption by using the mathematics of elliptic curves.

RSA does something similar with prime numbers instead of elliptic curves, but ECC has gradually been growing in popularity recently due to its smaller key size and ability to maintain security. This trend will probably continue as the demand on devices to remain secure increases due to the size of keys growing, drawing on scarce mobile resources. This is why it is so important to understand elliptic curve cryptography in context.

In contrast to RSA, ECC bases its approach to public key cryptographic systems on how elliptic curves are structured algebraically over finite fields. Therefore, ECC creates keys that are more difficult, mathematically, to crack. For this reason, ECC is considered to be the next generation implementation of public key cryptography and more secure than RSA.

It also makes sense to adopt ECC to maintain high levels of both performance and security. That's because ECC is increasingly in wider use as websites strive for greater online security in customer data and greater mobile optimization, simultaneously. More sites using ECC to secure data means a greater need for this kind of quick guide to elliptic curve cryptography.

An elliptic curve for current ECC purposes is a plane curve over a finite field which is made up of the points satisfying the equation:
$y^2=x^3 + ax + b$.

In this elliptic curve cryptography example, any point on the curve can be mirrored over the x-axis and the curve will stay the same. Any non-vertical line will intersect the curve in three places or fewer.

10.3 What is the zero point of an elliptic curve?

Even better, it allows us to define a group operation on E(Q), or on E(k), for any elliptic curve E defined over a field k. Three points on a line sum to zero. **Zero is the point at infinity**

10.4 What is the sum of three points on an elliptic curve that lie on a straight line?

Elliptic Curves - Graphs

Note

- Elliptic curves are not Ellipses
  - the graph of an ellipse looks like a flattened circle
  - equations for an elliptic curve are similar to those used to calculate the circumference of an ellipse

Elliptic Curves - Addition

A form of addition may be defined upon 'the set of points on an Elliptic curve E' such that an Abelian Group (E,+) results.

We begin with the following definition:

Definition

If three points lie on an elliptic curve E and at the same time also lie on a straight line then their sum is DEFINED to be '*0*' the *point at infinity* or *zero point* (see pp 193-195 of course text)

Elliptic Curves - Addition

- *0* is referred to as the additive identity. So
  - $P + 0 = 0$ and in particular $P + 0 = P$

Benefits or advantages of AES

https://binaryterms.com/advanced-encryption-standard-aes.html

Following are the benefits or advantages of AES:

➨As it is implemented in both hardware and software, it is most robust security protocol.

➨It uses higher length key sizes such as 128, 192, and 256 bits for encryption. Hence it makes AES algorithm more robust against hacking.

➨It is most common security protocol used for a wide variety of applications such as wireless communication, financial transactions, e-business, encrypted data storage, etc.

➨It is one of the most spread commercial and open source solutions used all over the world.

➨No one can hack your personal information.

➨For 128 bit, about 2^128 attempts are needed to break. This makes it very difficult to hack it as a result it is a very safe protocol.

Drawbacks or disadvantages of AES

Following are the disadvantages of AES:

➨It uses too simple an algebraic structure.

➨Every block is always encrypted in the same way.

➨Hard to implement with software.

➨AES in counter mode is complex to implement in software taking both performance and security into considerations.

Strength of DES

https://www.geeksforgeeks.org/strength-of-data-encryption-standard-des/
https://binaryterms.com/data-encryption-standard-des.html
https://www.educba.com/des-vs-aes/

Drawbacks of DES Algorithm

Any cipher who wants to decrypt the encrypted method has to use a brute force attack. A brute force attack is a way or mechanism in which several combinations are randomly applied to decrypt the message. In brute force, different combinations are applied one by one until it hits the right combination. Thus brute force works on the hit and trial method, where the intruder tries to hit again and again till he decrypts the message.

Generally, the length of this combination determines the number of possible combinations. For example, a DES uses 64 bits of encryption logic. Out of this available 64 bits, 8 bits are used for parity check. Hence effective bits now boils down to 56-bits only. These 56-bits apparently form a maximum combination of 2^56. Hence only 2^56 attempts are required to decrypt a message using brute force logic. This particular combination of hit and trial methods or brute force is quite low, which opens many vulnerabilities.

Hence this is the main reason why the DES algorithm was not practiced.

Substitution Technique in Cryptography

https://binaryterms.com/substitution-technique-in-cryptography.html

Transposition Technique in Cryptography

https://binaryterms.com/transposition-technique-in-cryptography.html