INFORMATION SECURITY

UNIT-I

IMPORTANCE OF INFORMATION SECURITY

Basic of Information System

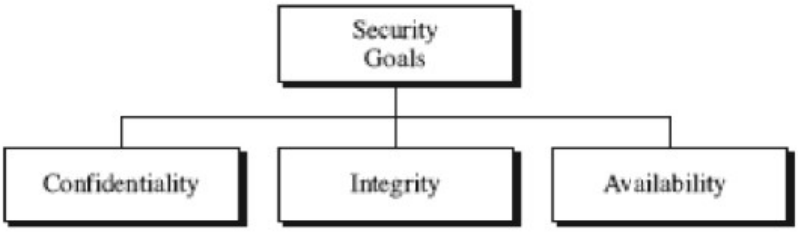
Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take electronic, print, or other forms.

Information systems (IS) is the study of complementary networks of hardware and software that people, and organizations use to collect, filter, process, create, and distribute data.

Information systems are combinations of hardware, software, and telecommunications networks that people build and use to collect, create, and distribute useful data, typically in organizational settings.

Security Goals

There are three primary goals in any security service. These are confidentially, integrity and availability.



Confidentiality

The principle of confidentiality is that only the sender and the intended recipient should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the message. Example of this could be a confidential email message sent by user A to user B, which is accessed by user C without the permission or knowledge of A and B. This type of attack is called interception.

Integrity

When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost. For example, consider that user A sends message to user B. User C tampers with a message originally sent by user A, which is actually destined for user B. User C somehow manages to access it, change its contents and send the changed message to user B. User B has no way of knowing that the contents of the message changed after user A had sent it. User A also does not know about this change. This type of attack is called modification.

Availability

The principle of availability is that resources should be available to authorized parties at all times. For example, due to the intentional actions of an unauthorized user C, an authorized user A may not be able to contact a server B. This would defeat the principle of availability. Such an attack is called interruption.

Techniques for Security Goal Implementation

The actual implementation of security goals needs some techniques. Two techniques are: one cryptography is very general and the other one steganography is specific.

Cryptography

Cryptography, a word with Greek origin, means "secret writing". However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. Although in the past cryptography referred only to the encryption and decryption of messages using secret keys, today it is defined as involving three distinct mechanisms: symmetric-key encipherment, asymmetric-key encipherment, and hashing. We will briefly discuss these three mechanisms here.

1. **Symmetric-key Encipherment**
   In symmetric encipherment, an entity, say Alice, can send a message to other entity, say Bob, over an insecure channel with the assumption that an adversary, say Eve, cannot understand the contents of the message by simply listen in over the channel. Alice encrypts the message using an encryption algorithm. Bob decrypts the message using a decryption algorithm. Symmetric-key encipherment uses a single secret key for both encryption and decryption. Encryption/decryption can be thought of as electronic locking system. In symmetric-key enciphering, Alice puts the message in a box and locks the box using the shared secret key; Bob unlocks the box with the same key and takes out the messages.
2. **Asymmetric Encipherment**
   In asymmetric encipherment, we have the same situation as the symmetric-key encipherment, with a few exceptions. First, there are two keys instead of one; one public key and one private key. To send a secure message to Bob, Alice firsts encrypts the message using Bob's public key. To decrypts the message, Bob uses his own private key.
3. **Hashing**
   Hashing is a mathematical operation that is easy to perform, but extremely difficult to reverse. (The difference between hashing and encryption is that encryption can be reversed, or decrypted, using a specific key.) The most widely used hashing functions are MD5, SHA1 and SHA-256. Some hashing processes are significantly harder to crack than others. For example, SHA1 is easier to crack than crypt.

Steganography

This is the art of hiding messages in another form. Message is not altered as in encryption. A text can hide a message. For example "red umbrella needed" may mean the message "run". The first letter of each word in the text becomes the message. An image can also be used for hiding messages. Digital images are after all binary information. Suppose the image is grey image. The least significant bit of consecutive eight pixel.

MATHEMATICAL BACKGROUND FOR CRYPTOGRAPHY

Cryptography

Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage. It is the practice of hiding information so that unauthorized persons can't read it. The literal meaning for cryptography is "hidden writing": how to make what you write obscure, unintelligible to everyone except whom you want to communicate with. Cryptography was already used in ancient times, essentially in three kinds of contexts: private communications, art and religion and military and diplomatic use.

Modular Arithmetic

Modular arithmetic is a system of arithmetic for integers, where values reset to zero and begin to increase again, after reaching a certain predefined value, called the modulus (*modulo*). Modular arithmetic is widely used in computer science and cryptography.

Greatest Common Divisor

The **greatest common divisor (GCD)**, also called the **greatest common factor**, of two numbers is the largest number that divides them both. For instance, the greatest common factor of 20 and 15 is 5, since 5 divides both 20 and 15 and no larger number has this property. The concept is easily extended to sets of more than two numbers: the GCD of a set of numbers is the largest number dividing each of them.

E.g.

Find the greatest common divisor of 30,36, and 24.

The divisors of each number are given by

30: 1,2,3,5,6,10,15,30

36: 1,2,3,4,6,9,12,18,36

24: 1,2,4,6,12,24

The largest number that appears on every list is 6,6, so this is the greatest common divisor:

gcd (30,36,24) = 6.

The Euclidean Algorithm

Recall that the Greatest Common Divisor (GCD) of two integers A and B is the largest integer that divides both A and B. The Euclidean Algorithm is a technique for quickly finding the GCD of two integers.

The Euclidean Algorithm for finding GCD (A, B) is as follows:

- If A = 0 then GCD (A, B) = B, since the GCD (0, B) = B, and we can stop.
- If B = 0 then GCD (A, B) = A, since the GCD (A, 0) = A, and we can stop.
- Write A in quotient remainder form (A = B·Q + R)

- Find GCD (B, R) using the Euclidean Algorithm since GCD (A, B) = GCD (B, R)

Example

Find the GCD of 270 and 192

- A=270, B=192
- A ≠0
- B ≠0
- Use long division to find that 270/192 = 1 with a remainder of 78. We can write this as: 270 = 192 * 1 +78
- Find GCD(192,78), since GCD(270,192)=GCD(192,78)

A=192, B=78

- A ≠0
- B ≠0
- Use long division to find that 192/78 = 2 with a remainder of 36. We can write this as:
- 192 = 78 * 2 + 36
- Find GCD(78,36), since GCD(192,78)=GCD(78,36)

A=78, B=36

- A ≠0
- B ≠0
- Use long division to find that 78/36 = 2 with a remainder of 6. We can write this as:
- 78 = 36 * 2 + 6
- Find GCD(36,6), since GCD(78,36)=GCD(36,6)

A=36, B=6

- A ≠0
- B ≠0
- Use long division to find that 36/6 = 6 with a remainder of 0. We can write this as:
- 36 = 6 * 6 + 0
- Find GCD(6,0), since GCD(36,6)=GCD(6,0)

A=6, B=0

- A ≠0
- B =0, GCD(6,0)=6

So we have shown:

GCD(270,192) = GCD(192,78) = GCD(78,36) = GCD(36,6) = GCD(6,0) = 6

GCD(270,192) = 6

Computing the Inverse

The *modular inverse* of an integer *e* modulo *n* is defined as the value of *d* such that ed = 1 mod n. We write d = (1/e) mod n or d = e^{-1} mod n. The inverse exists if and only if gcd (n, e) =1.

To find this value for large numbers on a computer, we use the extended Euclidean algorithm, but there are simpler methods for smaller numbers.

Trial and error

For very small numbers we can use trial and error. For example, to find the inverse of 3 modulo 20, we have e=3 and n=20 and we need to find the integer *d* such that when *ed* is divided by 20, the remainder is 1.

Try d=1, ed=3x1=3, 3 divided by 20 is 0 remainder 3, so no good

Try d=2, ed=3x2=6, 6 divided by 20 is 0 remainder 6, so no good

...

Try d=6, ed=3x6=18, 18 divided by 20 is 0 remainder 18, so no good

Try d=7, ed=3x7=21, 21 divided by 20 is 1 remainder 1 => HOORAY.

So d=7 satisfies the relationship. Therefore, a modular inverse d = 3^{-1} mod 20 = 7.

Using the Euclidean algorithm

If we need to find d = e^{-1} mod n and we can find integers *x* and *y* such that ex + ny = 1 then the inverse *d* is the value of *x*.

Using our method to find d = 3^{-1} mod 20, we first obtain gcd(20, 3) and check that it's one (otherwise the inverse doesn't exist).

20 = 3 x 6 + 2

3 = 2 x 1 + 1

giving gcd (20, 3) = 1. Then we use the numbers in this calculation to find Bezout's identity nx + ey = 1,

1 = 3 - 1 x 2

= 3 - 1 x (20 - 6 x 3)

= -1 x 20 + 7 x 3

The value of *x* (the coefficient of 3) is 7, so the inverse is 7

Extended Euclidean Algorithm

The extended Euclidean algorithm is an algorithm to compute integers *x* and *y* such that

ax + by = gcd(a,b)

given *a* and *b*.

The extended Euclidean algorithm can be viewed as the reciprocal of modular exponentiation.

By reversing the steps in the Euclidean algorithm, it is possible to find these integers x*x* and y*y*. The whole idea is to start with the GCD and recursively work our way backwards. This can be done by treating the numbers as variables until we end up with an expression that is a linear combination of our initial numbers. We shall do this with the example we used above.

Example

Find two integers *a* and *b* such that 1914a + 899b = gcd(1914,899).

First use Euclid's algorithm to find the GCD:

1914 =2×899+116

899 =7×116+87

116 = 1×87+29

87 = 3×29+0.

From this, the last non-zero remainder (GCD) is 2929. Now we use the extended algorithm:

29=116+(−1)×87

87 = 899+(−7)×116

Substituting for 8787 in the first equation, we have

29 =116+(−1)×(899+(−7)×116)

=(−1)×899+8×116

=(−1)×899+8×(1914+(−2)×899)

=8×1914+(−17)×899

=8×1914−17×899.

Since we now wrote the GCD as a linear combination of two integers, we terminate the algorithm and conclude

a=8,*b*=−17.

Fermat's Theorem

Fermat's little theorem states that if p is a prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p.

Here p is a prime number

$a^p \equiv a \pmod p$.

Special Case: If a is not divisible by p, Fermat's little theorem is equivalent to the statement that $a^{p-1}-1$ is an integer multiple of p.

Example

P = an integer Prime number

a = an integer which is not multiple of P

Let a = 2 and P = 17

According to Fermat's little theorem

$2^{17-1} \equiv 1 \bmod(17)$

we got $65536 \% 17 \equiv 1$

that mean (65536-1) is an multiple of 17.

Role of cryptography in information security

This investigation argues that cryptography is a very effective technique to protect highly confidential and valuable information from cyber criminals. Information security is becoming one of the hot topics around the world. The need for modern cryptography to provide techniques and keys to protect information is vital. The process of encryption and decryption is essential for the communication of highly sensitive information. This inquiry emphasizes that without cryptography, private information such as credit card details, passwords and identity card numbers will be accessible to cyber criminals. This study also discusses relevant topics such as the definitions of cryptography, history of cryptography, principles and types of cryptography. Even though cryptography is used to convert information into an unreadable format, we cannot be absolutely sure that confidential data would not be accessed by cyber criminals who seem to be getting smarter and smarter by the day. Technological advancements have enabled them to improve their criminal techniques.

Plain Text

Plaintext is a term used in cryptography that refers to a message before *encryption* or after *decryption*. That is, it is a message in a form that is easily readable by humans.

Plaintext is the term used to refer to the information in plain language that the sender desires to send to one or more receiving computers or individuals. Also referred to as cleartext, plaintext is commonly referred to as the input to a cipher or encryption algorithm. The term cleartext can also refer to sounds, images, or other multimedia information that is transmitted without encryption. In laymen's terms, plaintext refers to information that is represented in its "normal" form before any action is taken to conceal or compress the data.

Cipher Text

Cipher is an algorithm which is applied to plain text to get ciphertext. It is the unreadable output of an encryption algorithm. The term "cipher" is sometimes used as an alternative term for ciphertext. Ciphertext is not understandable until it has been converted into plain text using a key.

Key

A key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. This key remains private and ensures secure communication.

A key is the core part of cryptographic operations. Many cryptographic systems include pairs of operations, such as encryption and decryption. A key is a part of the variable data that is provided as input to a cryptographic algorithm to execute this sort of operation. In a properly designed cryptographic scheme, the security of the scheme is dependent on the security of the keys used.

Encryption

In computing, encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

Decryption

Decryption is generally the reverse process of encryption. It is the process of decoding the data which has been encrypted into a secret format. An authorized user can only decrypt data because decryption requires a

secret key or password.

Kerckhoffs's principle

Kerckhoffs's principle is one of the basic principles of modern cryptography. It was formulated in the end of the nineteenth century by Dutch cryptographer Auguste Kerckhoffs's. The principle goes as follows:

A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.

Kerckhoffs's principle is applied in virtually all contemporary encryption algorithms (DES, AES, etc.). These algorithms are considered to be secure and thoroughly investigated. The security of the encrypted message depends solely on the security of the secret encryption key (its quality).

The idea is that if any part of a cryptosystem (except the individual secret key) has to be kept secret then the cryptosystem is not secure. That's because if the simple act of disclosing some detail of the system were to make it suddenly insecure then you've got a problem on your hands.

A great example of this is the breaking of the Nazi German Enigma cipher during the Second World War. By stealing machines, receiving information from other secret services, and reading the manuals, the Allies knew everything there was to know about how the Enigma machine worked.

Substitution Cipher

Substitution ciphers are probably the most common form of cipher. They work by replacing each letter of the plaintext (and sometimes punctuation marks and spaces) with another letter (or possibly even a random symbol).

A *substitution cipher*, also known as a simple substitution cipher, relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the ciphertext.

A simple example is where each letter is encrypted as the next letter in the alphabet: "a simple message" becomes "B TJNQMF NFTTBHF". In general, when performing a simple substitution manually, it is easiest to generate the *ciphertext alphabet* first, and encrypt by comparing this to the plaintext alphabet. The table below shows how one might choose to, and we will, lay them out for this example.

Plaintext Alphabet	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
Ciphertext Alphabet	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	A

This key is then used identically to the example above. If your key word has repeated characters e.g. 'mammoth', be careful not to include the repeated characters in the cipher alphabet.

Transposition Ciphers

Transposition Ciphers are a bit different to Substitution Ciphers. Whereas Substitution ciphers replace each letter with a different letter or symbol to produce the ciphertext, in a Transposition cipher, the letters are just moved around.

The letters or words of the plaintext are reordered in some way, fixed by a given rule (the key).

One example of a transposition cipher is to reverse the order of the letters in a plaintext. So "a simple example" becomes "ELPMAXE ELPMIS A". Another, similar, way to encrypt a message would be to reverse the letters of each word, but not the order in which the words are written. In this case "a simple example" becomes "A ELPMIS ELPMAXE".

Types of Attacks on Ciphers

The basic intention of an attacker is to break a cryptosystem and to find the plaintext from the ciphertext. To obtain the plaintext, the attacker only needs to find out the secret decryption key, as the algorithm is already in public domain.

Hence, he applies maximum effort towards finding out the secret key used in the cryptosystem. Once the attacker is able to determine the key, the attacked system is considered as *broken* or *compromised*.

Based on the methodology used, attacks on cryptosystems are categorized as follows −

- **Ciphertext Only Attacks (COA)** − In this method, the attacker has access to a set of ciphertext(s). He does not have access to corresponding plaintext. COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext. Occasionally, the encryption key can be determined from this attack. Modern cryptosystems are guarded against ciphertext-only attacks.
- **Known Plaintext Attack (KPA)** − In this method, the attacker knows the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext using this information. This may be done by determining the key or via some other method. The best example of this attack is *linear cryptanalysis* against block ciphers.
- **Chosen Plaintext Attack (CPA)** − In this method, the attacker has the text of his choice encrypted. So he has the ciphertext-plaintext pair of his choice. This simplifies his task of determining the encryption key. An example of this attack is *differential cryptanalysis* applied against block ciphers as well as hash functions. A popular public key cryptosystem, RSA is also vulnerable to chosen-plaintext attacks.
- **Dictionary Attack** − This attack has many variants, all of which involve compiling a ‘dictionary’. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.

- **Brute Force Attack (BFA)** − In this method, the attacker tries to determine the key by attempting all possible keys. If the key is 8 bits long, then the number of possible keys is $2^8 = 256$. The attacker knows the ciphertext and the algorithm, now he attempts all the 256 keys one by one for decryption. The time to complete the attack would be very high if the key is long.

UNIT-II

INTRODUCTION TO CIPHERS

A cipher is a method of hiding words or text with encryption by replacing original letters with other letters, numbers and symbols through substitution or transposition. A combination of substitution and transposition is also often employed.

Monoalphabetic and polyalphabetic ciphers

A *monoalphabetic substitution cipher*, also known as a simple substitution cipher, relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the ciphertext.

A simple example is where each letter is encrypted as the next letter in the alphabet: "a simple message" becomes "B TJNQMF NFTTBHF". In general, when performing a simple substitution manually, it is easiest to generate the *ciphertext alphabet* first, and encrypt by comparing this to the plaintext alphabet. The table below shows how one might choose to, and we will, lay them out for this example.

Plaintext Alphabet	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
Ciphertext Alphabet	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	A

The development of **Polyalphabetic Substitution Ciphers** was the cryptographers answer to **Frequency Analysis**. The first known polyalphabetic cipher was the *Alberti Cipher* invented by Leon Battista Alberti in around 1467. He used a mixed alphabet to encrypt the plaintext, but at random points he would change to a different mixed alphabet, indicating the change with an uppercase letter in the ciphertext. In order to utilise this cipher, Alberti used a cipher disc to show how plaintext letters are related to ciphertext letters.

For example, when the disc on the left is set as shown, we see that the plaintext letter "e" (on the outside ring) is encrypted to "Z" (on the inside ring).

Perfect substitution cipher such as the Vernam cipher

The Vernam Cipher

Vernam Cipher is a method of encrypting alphabetic text. It is simply a type of substitution cipher. In this mechanism we assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, … z = 25).

Method to take key:

In Vernam cipher algorithm, we take a key to encrypt the plain text which length should be equal to the length of the plain text.

Algorithm

1. Assign a number to each character of the plain-text and the key according to alphabetical order.
2. Add both the number (Corresponding plain-text character number and Key character number).
3. Subtract the number from 26 if the added number is greater than 26. otherwise left it.

Example

Plain-Text: RAMSWARUPK

Key: RANCHOBABA

Now according to our encryption algorithm, we assign a number to each character of our plain-text and key.

PT: R A M S W A R U P K

NO: 17 0 12 18 22 0 17 20 15 10

KEY: R A N C H O B A B A

NO: 17 0 13 2 7 14 1 0 1 0

Now add the number of Plain-Text and Key and after doing the addition and subtraction operation (if required), we will get the corresponding Cipher-Text character number.

CT-NO: 34 0 25 20 29 14 18 20 16 10

In this case, there are two numbers which are greater than the 26 so we have to subtract 26 from them and after applying the subtraction operation the new Cipher text character numbers are as follow:

CT-NO: 8 0 25 20 3 14 18 20 16 10

New Cipher-Text is after getting the corresponding character from the number.

CIPHER-TEXT: I A Z U D O S U Q K

Stream and block cipher

A **block cipher** is an encryption algorithm that encrypts a fixed size of n-bits of data - known as a block - at one time. The usual sizes of each block are 64 bits, 128 bits, and 256 bits. So for example, a 64-bit block

cipher will take in 64 bits of plaintext and encrypt it into 64 bits of ciphertext. In cases where bits of plaintext are shorter than the block size, padding schemes are called into play.

A **stream cipher** is an encryption algorithm that encrypts 1 bit or byte of plaintext at a time. It uses an infinite stream of pseudorandom bits as the key. For a stream cipher implementation to remain secure, its pseudorandom generator should be unpredictable, and the key should never be reused. Stream ciphers are designed to approximate an idealized cipher, known as the One-Time Pad.

Let's see the difference between them:

S.NO	BLOCK CIPHER	STREAM CIPHER
1.	Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plaint text into cipher text by taking 1 byte of plain text at a time.
2.	Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
3.	The complexity of block cipher is simple.	While stream cipher is more complex.
4.	Block cipher Uses confusion as well as diffusion.	While stream cipher uses only confusion.
5.	In block cipher, reverse encrypted text is hard.	While in stream cipher, reverse encrypted text is easy.
6.	The algorithm modes which are used in block cipher are: ECB (Electronic Code Book) and CBC (Cipher Block Chaining).	The algorithm modes which are used in stream cipher are: CFB (Cipher Feedback) and OFB (Output Feedback).

Confusion and Diffusion

Diffusion means that if we change a character of the plaintext, then several characters of the ciphertext should change, and similarly, if we change a character of the ciphertext, then several characters of the plaintext should change.

Confusion means that the key does not relate in a simple way to the ciphertext. In particular, each character of the ciphertext should depend on several parts of the key.

S.NO	CONFUSION	DIFFUSION
1.	Confusion is a cryptographic technique which is used to create faint cipher texts.	While diffusion is used to create cryptic plain texts.
2.	This technique is possible through substitution algorithm.	While it is possible through transportation algorithm.
3.	In confusion, if one bit within the secret's modified, most or all bits within the cipher text also will be modified.	While in diffusion, if one image within the plain text is modified, many or all image within the cipher text also will be modified
4.	In confusion, vagueness is increased in resultant.	While in diffusion, redundancy is increased in resultant.
5.	Both stream cipher and block cipher use confusion.	Only block cipher uses diffusion.
6.	The relation between the cipher text and the key is masked by confusion.	While The relation between the cipher text and the plain text is masked by diffusion.

Unicity Distance

In cryptography, unicity distance is the length of an original ciphertext needed to break the cipher by reducing the number of possible spurious keys to zero in a brute force attack. That is, after trying every possible key, there should be just one decipherment that makes sense, i.e. expected amount of ciphertext needed to determine the key completely, assuming the underlying message has redundancy.

Consider an attack on the ciphertext string "WNAIW" encrypted using a Vigenère cipher with a five-letter key. Conceivably, this string could be deciphered into any other string—RIVER and WATER are both possibilities for certain keys. This is a general rule of cryptanalysis: with no additional information it is impossible to decode this message.

Of course, even in this case, only a certain number of five letter keys will result in English words. Trying all possible keys, we will not only get RIVER and WATER, but SXOOS and KHDOP as well. The number of "working" keys will likely be very much smaller than the set of all possible keys. The problem is knowing which of these "working" keys is the right one; the rest are spurious.

CRYPTANALYSIS

Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text. Cryptanalysis uses mathematical formulas to search for algorithm vulnerabilities and break into cryptography or information security systems.

Cryptanalysis is defined as the process of attempting to find a shortcut method, not envisioned by the designer, for decrypting an enciphered message when the key used to encrypt the message is not known.

Cryptanalysis of Monoalphabetic Ciphers such as Affine Cipher

The Affine Cipher is an example of Monoalphabetic Substitution Cipher. It is slightly different to the others, since the encryption process is substantially mathematical. The whole process relies on working *modulo m* (the length of the alphabet used). By performing a calculation on the plaintext letters, we encipher the plaintext.

Encryption

The first step in the encryption process is to transform each of the letters in the plaintext alphabet to the corresponding integer in the range 0 to *m*-1. With this done, the encryption process for each letter is given by

$E(x) = (ax + b) \bmod m$

where *a* and *b* are the key for the cipher. This means that we multiply our integer value for the plaintext letter by *a*, and then add *b* to the result. Finally, we take this modulus *m* (that is we take the remainder when the solution is divided by *m*, or we take away the length of the alphabet until we get a number less than this length).

As an example, let us encrypt the plaintext "affine cipher", using the key $a = 5$, $b = 8$. Firstly, we must find the integer value of each of the letters in the plaintext alphabet (the standard alphabet of 26 letters in this case). The table below gives these values.

Plaintext Alphabet	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
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

With the integer values of the plaintext letters found, the next step is to perform the calculations on those values. In this instance, the calculation needed is (5x+8). Finally, we must ensure that all our answers are calculated mod 26 and convert the integers back to ciphertext letters. All this information is shown in the table below.

Plaintext	a	f	f	i	n	e		c	i	p	h	e	r
x	0	5	5	8	13	4		2	8	15	7	4	17
5x+8	8	33	33	48	73	28		18	48	83	43	28	93
(5x+8) mod 26	8	7	7	22	21	2		18	22	5	17	2	15
Ciphertext	I	H	H	W	V	C		S	W	F	R	C	P

Thus the ciphertext produced is "IHHWVC SWFRCP".

Decryption

In deciphering the ciphertext, we must perform the opposite (or inverse) functions on the ciphertext to retrieve the plaintext. Once again, the first step is to convert each of the ciphertext letters into their integer values. We must now perform the following calculation on each integer

$\mathbf{D(x) = c(x - b) \bmod m}$

where c is the modular multiplicative inverse of a. That is, $a \times c = 1 \bmod m$ (c is the number such that when you multiply a by it, and keep taking away the length of the alphabet, you get to 1).

Continuing our example, we shall decrypt the ciphertext "IHHWVC SWFRCP", using a key of $a = 5$, $b = 8$. The first step here is to find the inverse of a, which in this case is 21 (since 21 x 5 = 105 = 1 mod 26, as 26 x 4 = 104, and 105 - 104 = 1). We must now perform the inverse calculations on the integer values of the ciphertext. In this case the calculation in $21(y - 8)$. Once again, we must take these answers modulo 26, and finally convert the integers back to plaintext letters. This is shown in the table below.

Ciphertext	I	H	H	W	V	C		S	W	F	R	C	P
y	8	7	7	22	21	2		18	22	5	17	2	15
21(y - 8)	0	-21	-21	294	273	-126		210	294	-63	189	-126	147
21(y - 8) mod 26	0	5	5	8	13	4		2	8	15	7	4	17
Plaintext	a	f	f	i	n	e		c	i	p	h	e	r

The decryption process for a key of a = 5, b = 8. We had to find the inverse of a first, which is 21.

We retrieve our plaintext of "affine cipher".

For more information visit: https://crypto.interactive-maths.com/affine-cipher.html

Cryptanalysis of Polyalphabetic Ciphers such as Vigenere Cipher

What is today known as the Vigenère Cipher was actually first described by Giovan Battista Bellaso in his 1553 book *La cifra del. Sig. Giovan Battista Bellaso*. However, in the 19th Century, it was misattributed to Blaise de Vigenère, who had presented a similar cipher (the **Autokey Cipher**) in 1586.

At the time, and for many centuries since its invention, the Vigenère Cipher was renowned for being a very secure cipher, and for a very long time it was believed to be unbreakable. It was this thought that earned it the nickname "le chiffre indéchiffrable" (French for "the unbreakable cipher"). Although this is not true (it was fully broken by Friedrich Kasiski in 1863), it is still a very secure cipher in terms of paper and pen methods, and is usable as a field cipher.

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

Encryption

To encrypt a message using the Vigenère Cipher you first need to choose a keyword (or keyphrase). You then repeat this keyword over and over until it is the same length as the plaintext. This is called the *keystream*.

Now for each plaintext letter, you find the letter down the left hand side of the tabula recta. You also take the corresponding letter from the keystream, and find this across the top of the tabula recta. Where these two lines cross in the table is the ciphertext letter you use.

Decryption

To decrypt a ciphertext with the keyword, we first have to generate the keystream by repeating the keyword until we have a keystream the same length as the ciphertext. Then you find the column with the letter of the keystream at the top, and go down this column until you find the ciphertext letter. Now read across to the far left of the table to reveal the plaintext letter.

More Details: https://crypto.interactive-maths.com/vigenegravere-cipher.html

UNIT-III

PUBLIC KEY (ASYMMETRIC KEY) ENCRYPTION SYSTEMS

Asymmetrical encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It ensures that malicious persons do not misuse the keys. It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boosting security. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know.

A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.

Concept and characteristics of public key encryption system

Confidentiality - because the content is encrypted with an individual's public key, it can only be decrypted with the individual's private key, ensuring only the intended recipient can decrypt and view the contents.

Integrity - part of the decryption process involves verifying that the contents of the original encrypted message and the new decrypted match, so even the slightest change to the original content would cause the decryption process to fail.

Authentication – since the individual's unique private key was used to apply the signature, recipients can be confident that the individual was the one to actually apply the signature.

Introduction to Merkle-Hellman Knapsacks

Rivest–ShamirAdlman (RSA) Encryption

DIGITAL SIGNATURE

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

Introduction to digital signature algorithms

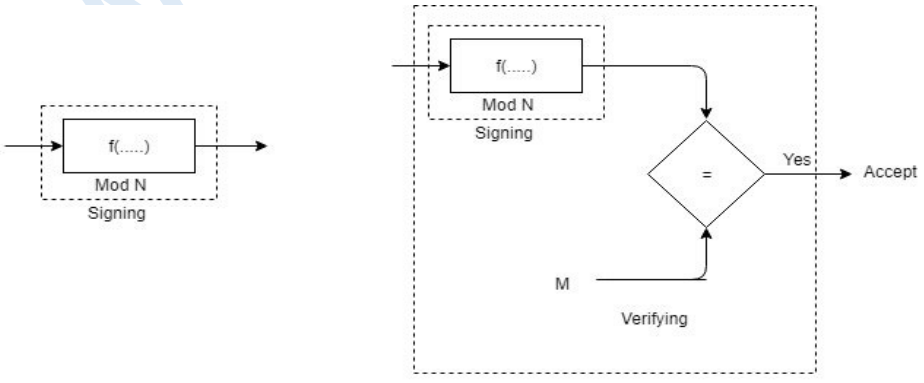
As we have already seen, DSA is one of the many algorithms that are used to create digital signatures for data transmission. In DSA, a pair of numbers is created and used as a digital signature. These are generated using some specific algorithms. They allow the receiver to authenticate the origin of the message. The digital signature, created using DSA, is in private at the starting point of the data transmission, while ends in public. What this means is that only the person transmitting the data can make the signature, which is to be added to the message, but anyone can authenticate the signature at the other end.

Digital signatures are work on the principle of two mutually authenticating cryptographic keys. Signatures are based on public/private key pairs. With public key algorithm like RSA, one can create a mathematically linked private key and public key. One can sign a digital message with his private key. Signature related data can be encrypted by a person with the use of a private key. The private key should always be with a person who wants to create a digital signature. The public and the private key, both can always be derived from one another as they are related mathematically. Signer's public key is the only way to decrypt this data. One can give the public key to anyone who needs verification of the signer's signature. It is vital to keep private key secret as one can generate your signature on a document with the help of this. In this manner, the authentication digital signature is done. In a digital signature, validly is only assured by public and private keys.

On the other hand, the digital signature algorithm does not use a private key to encrypt data. Also, a digital signature algorithm does use a public key to decrypt this data. To create a digital signature with two 160-bit numbers, DSA works on the principle of a unique mathematical function. These two numbers are made by using the private key and the message digest.

RSA (Rivest–Shamir–Adleman) digital signature scheme algorithm

- RSA idea is also used for signing and verifying a message it is called RSA digital signature scheme.
- Digital signature scheme changes the role of the private and public keys
- Private and public keys of only the sender are used not the receiver
- Sender uses her own private key to sign the document and the receiver uses the sender's public key to verify it.



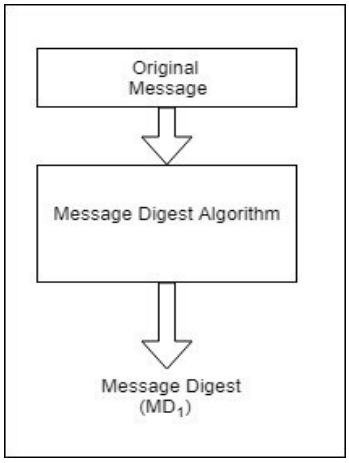
General Ideal behind RSA Digital Signature Sceme

- The signing and verifying sets use the same function, but with different parameters. The verifier compares the message and the output of the function for congruence. If the result is two true, the message is accepted.

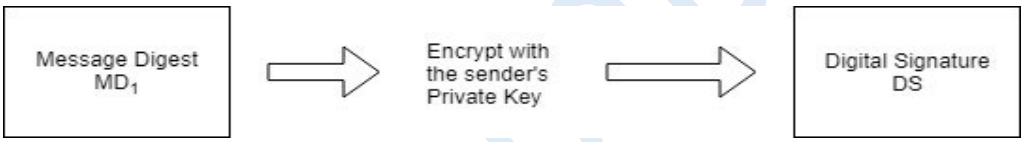
Working of RSA digital signature scheme:

Sender A wants to send a message M to the receiver B along with the digital signature S calculated over the message M

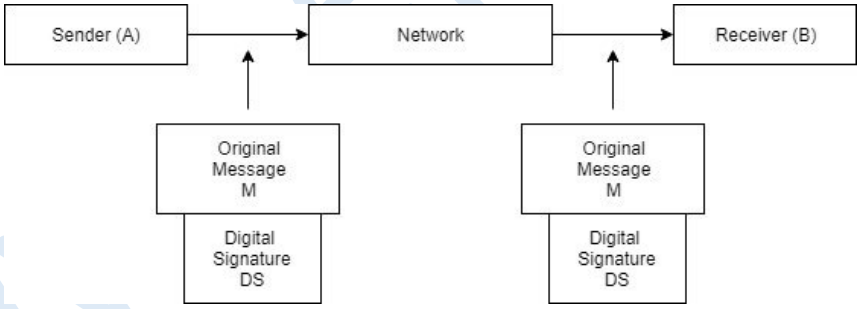
Step1: The sender A uses the message digest algorithm to calculate the message digest MD1 over the original message M



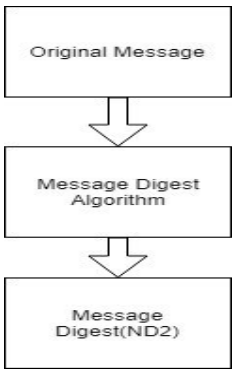
Step 2: The sender A now encrypts the message digest with her private key. The output of this process is called the digital signature.



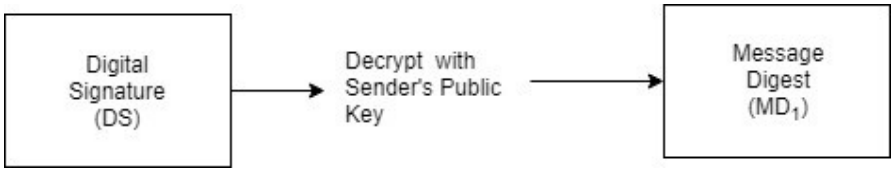
Step 3: Now the sender A sends the original message M along with digital signature DS to receiver B



Step 4: After the receiver B receives the original message M and the sender A's digital signature, B uses the same message digest algorithm which was used by A and calculate its own message digest MD2 as shown below.



Step 5: The receiver B now uses the sender's A's public key to decrypt the digital signature. Note that A had used his private key to decrypt the message digest MD1 to form the digital signature. Therefore, only A's public key can be used to decrypt it. The output of this process is the original message digest which was calculated by A (MD1) in step 1.



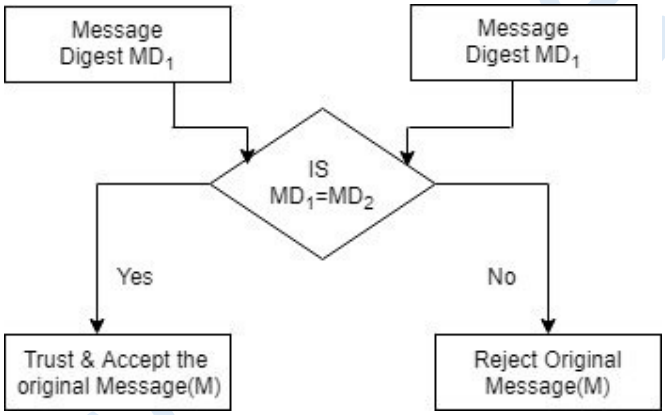
Step 6: B now compare the following two message digests.

1. MD2, which it had calculated in step 4
2. MD1, which is retrieved from A's digital signature in step 5

If MD1 = MD2 the following facts are established:

a. B accepts the original message (M) as the correct, unaltered message from A

b. B is also assured that the message came from A and not from someone else attached, posing as A



Thus, the principle of digital signature is quite strong, secure and reliable.

Digital Signature Standard

Developed by the U.S. National Security Agency, the Digital Signature Standard (DSS) is a collection of procedures and standards for generating a digital signature used for authenticating electronic documents. Specified as Federal Information Processing Standard 186 by the National Institute of Standards and Technology (NIST) in 1994, the Digital Signature Standard has become the U.S. government standard for authenticating electronic documents.

The Digital Signature Standard is intended to be used in electronic funds transfer, software distribution, electronic mail, data storage and applications which require high data integrity assurance. The Digital Signature Standard can be implemented in software, hardware or firmware.

The Digital Signature Standard ensures that the digital signature can be authenticated and the electronic documents carrying the digital signatures are secure. The standard also ensures non-repudiation with regards to the signatures and provides all safeguards for imposter prevention. The standard also ensures that digital signed documents can be tracked.

UNIT-IV

SECURE SECRET KEY (SYMMETRIC) SYSTEMS

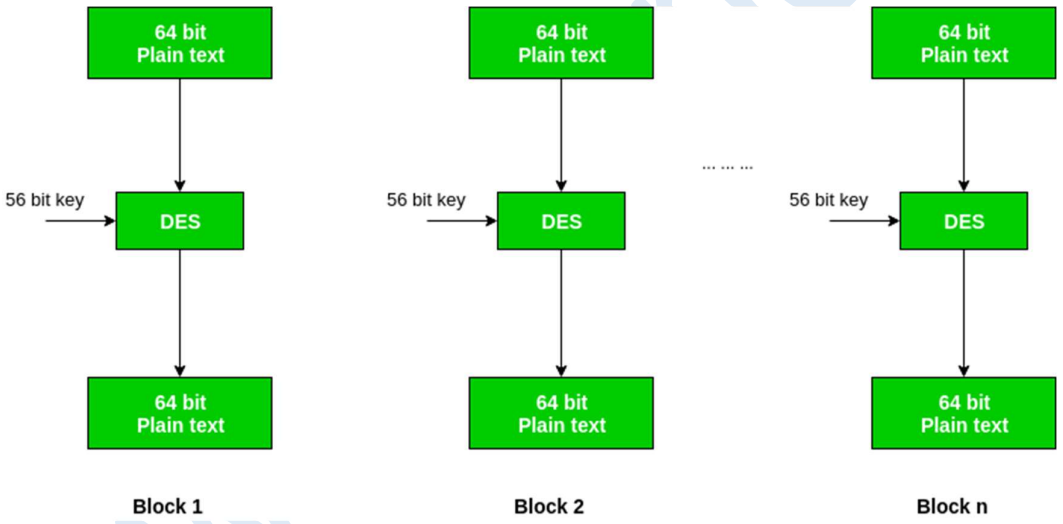
Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages.

By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it. Once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original and understandable form.

Data Encryption Standard (DES)

Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline.

DES is a block cipher and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. The basic idea is show in figure.



We have mention that DES uses a 56-bit key. Actually, the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit position 8, 16, 24, 32, 40, 48, 56 and 64 are discarded.

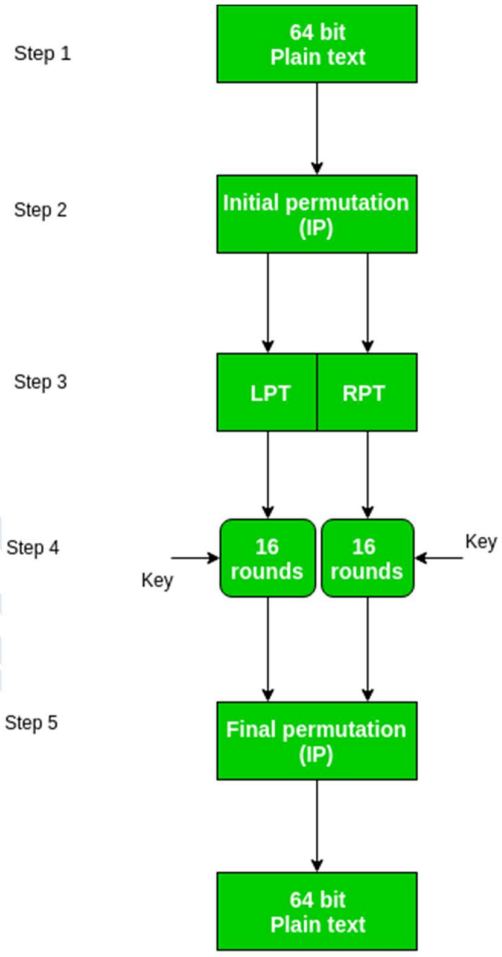
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

Figure - discording of every 8th bit of original key

Thus, the discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key.

DES is based on the two fundamental attributes of cryptography: substitution (also called as confusion) and transposition (also called as diffusion). DES consists of 16 steps, each of which is called as a round. Each round performs the steps of substitution and transposition.

1. In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.
2. The initial permutation performed on plain text.
3. Next the initial permutation (IP) produces two halves of the permuted block; says Left Plain Text (LPT) and Right Plain Text (RPT).
4. Now each LPT and RPT to go through 16 rounds of encryption process.
5. In the end, LPT and RPT are re-joined and a Final Permutation (FP) is performed on the combined block
6. The result of this process produces 64-bit cipher text.



Initial Permutation (IP)

As we have noted, the Initial permutation (IP) happens only once and it happens before the first round. It suggests how the transposition in IP should proceed, as show in figure.

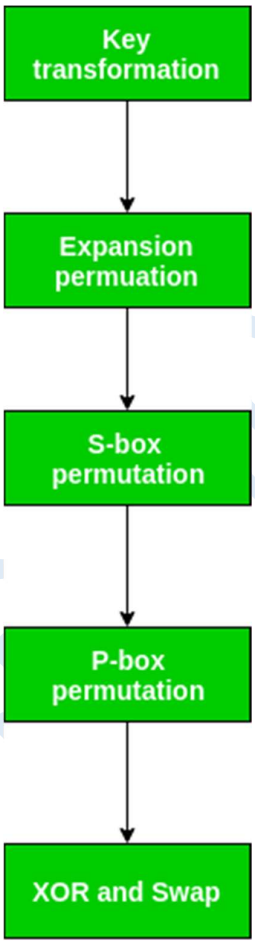
For example, it says that the IP replaces the first bit of the original plain text block with the 58th bit of the original plain text, the second bit with the 50th bit of the original plain text block and so on.

This is nothing but jugglery of bit positions of the original plain text block. the same rule applies for all the other bit positions which shows in the figure.

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	33	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Figure - Initial permutation table

As we have noted after IP done, the resulting 64-bit permuted text block is divided into two half blocks. Each half block consists of 32 bits, and each of the 16 rounds, in turn, consists of the broad level steps outlined in figure.



Step-1: Key transformation

We have noted initial 64-bit key is transformed into a 56-bit key by discarding every 8th bit of the initial key. Thus, for each a 56-bit key is available. From this 56-bit key, a different 48-bit Sub Key is generated during each round using a process called as key transformation. For this the 56 bit key is divided into two halves, each of 28 bits. These halves are circularly shifted left by one or two positions, depending on the round.

For example, if the round number 1, 2, 9 or 16 the shift is done by only position for other rounds, the circular shift is done by two positions. The number of key bits shifted per round is show in figure.

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
#key bits shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Figure - number of key bits shifted per round

After an appropriate shift, 48 of the 56 bits are selected. for selecting 48 of the 56 bits the table show in figure given below. For instance, after the shift, bit number 14 moves on the first position, bit number 17 moves on the second position and so on. If we observe the table carefully, we will realize that it contains only 48-bit positions. Bit number 18 is discarded, like 7 others, to reduce a 56-bit key to a 48-bit key. Since the key transformation process involves permutation as well as selection of a 48-bit sub set of the original 56-bit key it is called Compression Permutation.

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Figure - compression permutation

Because of this compression permutation technique, a different subset of key bits is used in each round. That's make DES not easy to crack.

Step-2: Expansion Permutation

Recall that after initial permutation, we had two 32-bit plain text areas called as Left Plain Text (LPT) and Right Plain Text (RPT). During the expansion permutation, the RPT is expanded from 32 bits to 48 bits. Bits are permuted as well hence called as expansion permutation. This happens as the 32-bit RPT is divided into 8 blocks, with each block consisting of 4 bits. Then, each 4-bit block of the previous step is then expanded to a corresponding 6-bit block, i.e., per 4 bit block, 2 more bits are added.

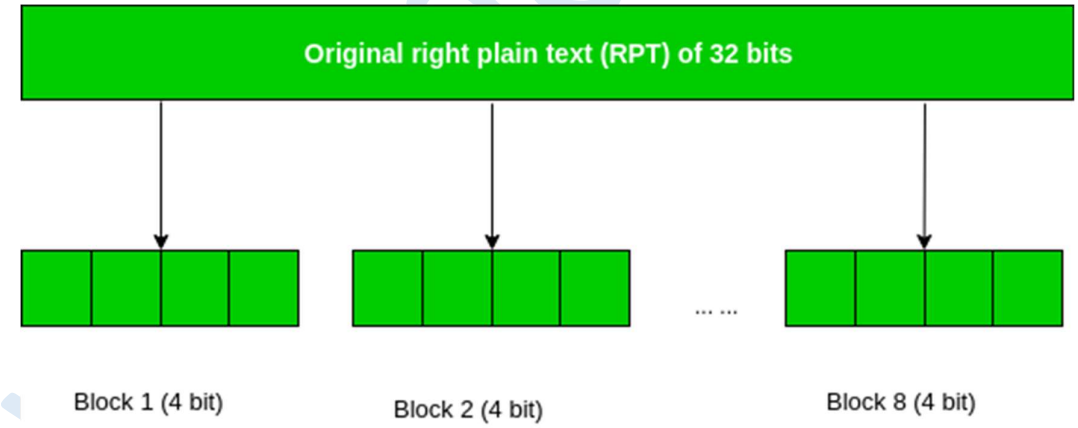


Figure - division of 32 bit RPT into 8 bit blocks

This process results into expansion as well as permutation of the input bit while creating output. Key transformation process compresses the 56-bit key to 48 bits. Then the expansion permutation process expands the 32-bit RPT to 48-bits. Now the 48-bit key is XOR with 48-bit RPT and resulting output is given to the next step, which is the S-Box substitution.

Introduction to Advance Encryption Standard (AES).

AES encryption uses a single key as a part of the encryption process. The key can be 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes) in length. The term 128-bit encryption refers to the use of a 128-bit encryption key. With AES both the encryption and the decryption are performed using the same key. This is called a symmetric encryption algorithm. Encryption algorithms that use two different keys, a public and a private key, are called asymmetric encryption algorithms.

An encryption key is simply a binary string of data used in the encryption process. Because the same encryption key is used to encrypt and decrypt data, it is important to keep the encryption key a secret and to use keys that are hard to guess. Some keys are generated by software used for this specific task. Another method is to derive a key from a pass phrase. Good encryption systems never use a pass phrase alone as an encryption key

Modes of Operation

There are different methods of using keys with the AES encryption method. These different methods are called “modes of operation”. NIST (National Institute of Standards and Technology) defines a number of modes of operation for AES which include:

- Electronic code book (ECB)
- Cipher block chaining (CBC)
- Counter (CTR)
- Cipher feed-back (CFB)
- Output feed-back (OFB)
- Galois Counter Mode (GCM)

Each mode uses AES in a different way. For example, ECB encrypts each block of data independently. CTR mode encrypts a 128-bit counter and then adds that value to the data to encrypt it. CBC mode uses an initialization vector and adds the encrypted value of each block to the data in the next block before encrypting it. Some modes require you to only encrypt data that is a multiple of the 16-byte block size; others allow you to truncate unused data.

Key Management

Many people think that encryption is all about secret methods, or algorithms, for obscuring code. In reality the encryption methods are public, and anyone can read how encryption is done and obtain source code for performing the encryption and decryption steps. The secret part is the key used to perform encryption and decryption. For this reason, it is important to keep your encryption keys secret, and use secure methods for creating, distributing, and storing your keys.

Key management systems allow you to create keys and keep them secret. Many security professionals believe that the most important part of their data security strategy is the proper creation, management, and protection of their encryption keys.

Difference between AES and DES ciphers

AES and DES are both examples of symmetric block ciphers but have certain dissimilarities.

AES	DES
AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard
Key length can be of 128-bits, 192-bits and 256-bits.	Key length is 56 bits in DES.
Number of rounds depends on key length: 10(128-bits), 12(192-bits) or 14(256-bits)	DES involves 16 rounds of identical operations
The structure is based on substitution-permutation network.	The structure is based in feistal network.
AES is more secure than the DES cipher and is the de facto world standard.	DES can be broken easily as it has known vulnerabilities. 3DES (Triple DES) is a variation of DES which is secure than the usual DES.
The rounds in AES are: Byte Substitution, Shift Row, Mix Column and Key Addition	The rounds in DES are: Expansion, XOR operation with round key, Substitution and Permutation
AES can encrypt 128 bits of plaintext.	DES can encrypt 64 bits of plaintext.
AES cipher is derived from square cipher.	DES cipher is derived from Lucifer cipher.
AES was designed by Vincent Rijmen and Joan Daemen.	DES was designed by IBM.
No known crypt-analytical attacks against AES but side channel attacks against AES implementations possible. Biclique attack have better complexity than brute-force but still ineffective.	Known attacks against DES include: Brute-force, Linear cryptanalysis and Differential cryptanalysis.

LAW AND LEGAL FRAMEWORK

Information is an important tool for successful organisations and Information Security Law forms a key part of that equation. Information Security Law is the body of legal rules, codes, and standards that require you to protect that information and the information systems that process it, from unauthorized access. The legal risks are potentially significant if you don't take a pragmatic approach.

Information security and law

Securing information is about securing value. In the same way that we secure physical stores of value such

as cash, gold, or jewellery against theft, loss, or destruction, we must do the same with digital stores of value – particularly information. We live in an information society, after all, where the creation, use, and distribution of information is a significant economic, political, and cultural activity. We are moving from the service economy into the information economy, which emphasizes informational activities that rely on information technologies such as computers, mobile devices, and the Internet.

The Indian IT act

In this Act, unless the context otherwise requires:

(a) Access with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

(b) Addressee means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(c) Adjudicating officer‖ means an adjudicating officer appointed under sub-section (1) of section 46;

(d) Affixing (electronic signature) with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

Objectives of the Act

The objectives of the Act are as follows:

i. Grant legal recognition to all transactions done via electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication.

ii. Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication

iii. Facilitate the electronic filing of documents with Government agencies and also departments

iv. Facilitate the electronic storage of data

v. Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions

vi. Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

Features of the Information Technology Act, 2000

a. All electronic contracts made through secure electronic channels are legally valid.

b. Legal recognition for digital signatures.

c. Security measures for electronic records and also digital signatures are in place

d. A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized

e. Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.

f. An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court

g. Digital Signatures will use an asymmetric cryptosystem and also a hash function

Copyright Law

Copyright is a legal term describing ownership of control of the rights to the use and distribution of certain works of creative expression, including books, video, movies, music and computer programs. Historically, copyright law has been enacted to balance the desire of cultures to use and reuse creative works (thus creating "derivative work") against the desire of the creators of art, literature, music and the like to monetize their work by controlling who can make and sell copies of the work.

Generally speaking, the copyright in a work protects its specific form, rather than the ideas suggested by or underlying the work. Originally intended to protect creative works of art and literature, copyright is one of the easiest and best ways to protect computer software.

The prerequisite for all works is that they be "original". The work must have been created by the author and not copied. As the name suggests, "work" (referred to in the case law as "effort") must be expended by the author to create the "work" in which copyright subsists.

Indian Copyright Law

Copyright is a form of intellectual property protection granted under Indian law to the creators of original works of authorship such as literary works (including computer programs, tables and compilations including computer databases which may be expressed in words, codes, schemes or in any other form, including a machine readable medium), dramatic, musical and artistic works, cinematographic films and sound recordings.

Copyright law protects expressions of ideas rather than the ideas themselves. Under section 13 of the Copyright Act 1957, copyright protection is conferred on literary works, dramatic works, musical works, artistic works, cinematograph films and sound recording. For example, books, computer programs are protected under the Act as literary works.

In India, the registration of copyright is not mandatory as the registration is treated as mere recordal of a fact. The registration does not create or confer any new right and is not a prerequisite for initiating action against infringement. The view has been upheld by the Indian courts in a catena of judgments.

Privacy on Internet

Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences.

Internet privacy is cause for concern for any user planning to make an online purchase, visit a social networking site, participate in online games or attend forums. If a password is compromised and revealed, a victim's identity may be fraudulently used or stolen.

Understanding Ethical Hacking

Ethical hacking is terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the system security, to minimize or eliminate any potential attacks.

The purpose of ethical hacking is to evaluate the security of and identify vulnerabilities in systems, networks or system infrastructure. It includes finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible.

Social Engineering Issue

Social engineering is the art of manipulating people, so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Ethical Domain for Information Security