Roll #.15375 Student Name Kifayat Ullah

IQRA NATIONAL UNIVERSITY, PESHAWAR, PAKISTAN

ADVANCE NETWORK SECURITY

Program: MSCS	**Final Term Exam**	**Semester: Summer-2020**
Maximum Marks: 50		**Time Allowed: 4 Hour**

Q1. What is meant by DES? Describe its history with Encryption Techniques Overview. Also describe its DES Round structure with substitution boxes overview.

Answer: **DES**: -

The data encryption standard (DES) is a common standard for data encryption and a form of secret key cryptography (SKC), which uses only one key for encryption and decryption. Public key cryptography (PKC) uses two keys, i.e., one for encryption and one for decryption.

DES History with encryption Technique

Up until recently, the main standard for encrypting data was a symmetric algorithm known as the Data Encryption Standard (DES). However, this has now been replaced by a new standard known as the Advanced Encryption Standard (AES) which we will look at later. DES is a 64-bit block cipher which means that it encrypts data 64 bits at a time. This is contrasted to a stream cipher in which only one bit at a time (or sometimes small groups of bits such as a byte) is encrypted.

DES was the result of a research project set up by International Business Machines (IBM) corporation in the late 1960's which resulted in a cipher known as LUCIFER. In the early 1970's it was decided to commercialize LUCIFER and a number of significant changes were introduced. IBM was not the only one involved in these changes as they sought technical advice from the National Security Agency (NSA) (other outside consultants were involved but it is likely that the NSA were the major contributors from a technical point of view). The altered version of LUCIFER was put forward as a proposal for the new national encryption standard requested by the National Bureau of Standards (NBS). It was finally adopted in 1977 as the Data Encryption Standard - DES (FIPS PUB 46).

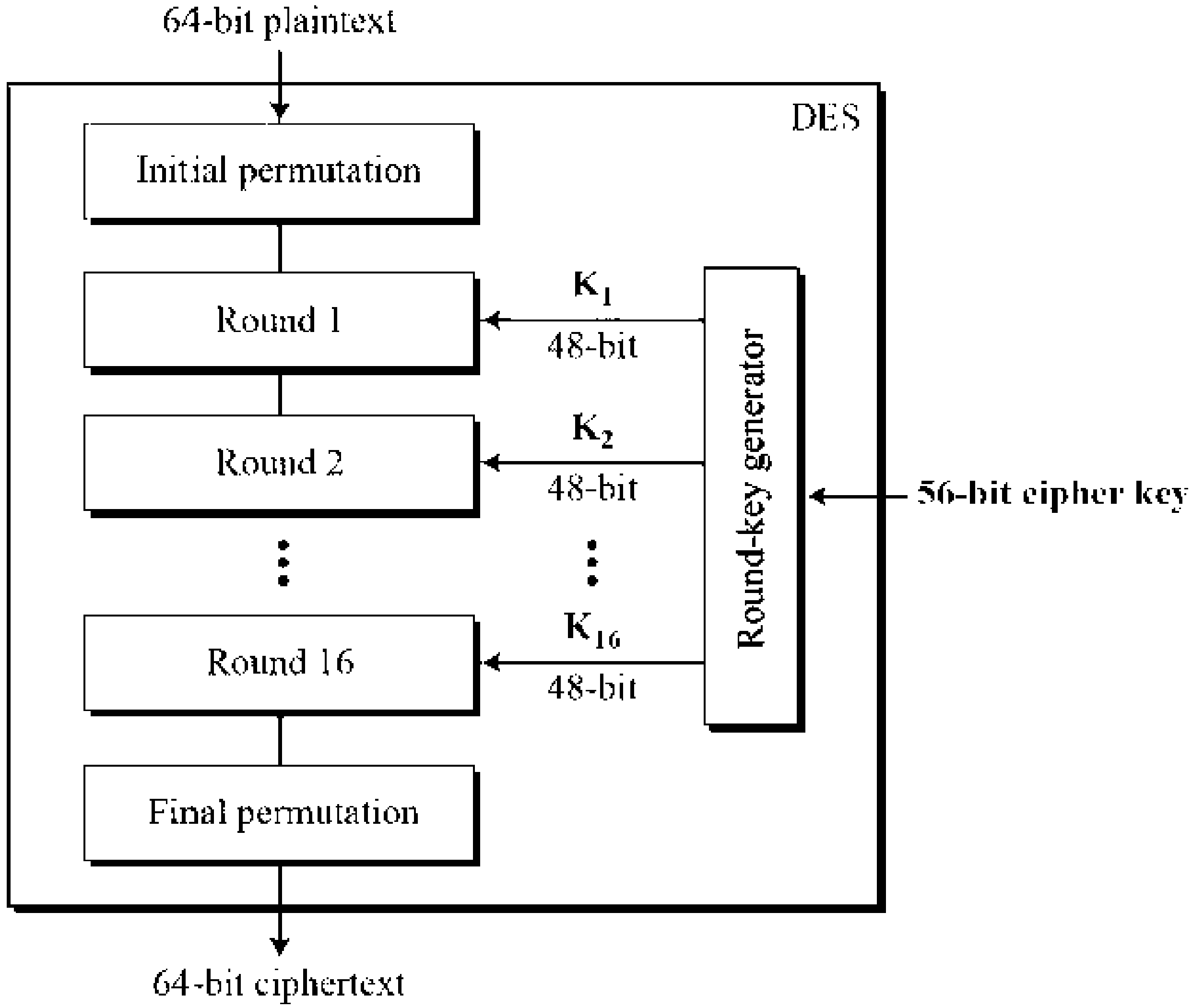
Some of the changes made to LUCIFER have been the subject of much controversy even to the present day. The most notable of these was the key size. LUCIFER used a key size of 128 bits however this was reduced to 56 bits for DES. Even though DES actually accepts a 64-bit key as input, the remaining eight bits are used for parity checking and have no effect on DES's security. Outsiders were convinced that the 56-bit key was an easy target for a brute force attack due to its extremely small size. The need for the parity checking scheme was also questioned without satisfying answers

Another controversial issue was that the S-boxes used were designed under classified conditions and no reasons for their particular design were ever given. This led people to assume that the NSA had introduced a “trapdoor” through which they could decrypt any data encrypted by DES even without knowledge of the key. One startling discovery was that the S-boxes appeared to be secure against an attack known as Differential Cryptanalysis which was only publicly discovered by Biham and Shamir in 1990. This suggests that the NSA were aware of this attack in 1977; 13 years earlier! In fact the DES designers claimed that the reason they never made the design specifications for the S-boxes available was that they knew about a number of attacks that weren’t public.knowledge at the time and they didn’t want them leaking - this is quite a plausible claim as differential cryptanalysis has shown. However, despite all this controversy, in 1994 NIST reformed DES for government use for a further five years for use in areas other than “classifed”.

DES of course isn’t the only symmetric cipher. There are many others, each with varying levels of complexity. Such ciphers include: IDEA, RC4, RC5, RC6 and the new Advanced Encryption Standard (AES). AES is an important algorithm and was originally meant to replace DES (and its more secure variant triple DES) as the standard algorithm for non-classi?ed material. However as of 2003, AES with key sizes of 192 and 256 bits has been found to be secure enough to protect information up to top secret. Since its creation, AES had underdone intense scrutiny as one would expect for an algorithm that is to be used as the standard. To date it has withstood all attacks but the search is still on and it remains to be seen whether or not this will last. We will look at AES later in the course.

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration −



Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

Rounds DES uses 16 rounds. Each round of DES is a Feistel cipher, as shown in Fig. 6.4. Swapper Mixer Round KI LI–1 LI RI–1 RI 32 bits 32 bits 32 bits 32 bits f (RI–1, KI) Fig. 6.4 A round in DES (encryption site) The round takes LI−1 and RI−1 from previous round (or the initial permutation box) and creates LI and RI , which go to the next round (or final permutation box). As we discussed in Chapter 5, we can assume that each round has two cipher elements (mixer and swapper). Each of these elements is invertible. The swapper is obviously invertible. It swaps the left half of the text with the right half. The mixer is invertible because of the XOR operation. All noninvertible elements are collected inside the function f (RI−1, KI

In cryptography, an **S-box** (**substitution-box**) is a basic component of symmetric key algorithms which performs substitution. In block ciphers, they are typically used to obscure the relationship between the key and the ciphertext — Shannon's property of confusion.

In general, an S-box takes some number of input bits, *m*, and transforms them into some number of output bits, *n*, where *n* is not necessarily equal to *m*.[1] An *m*×*n* S-box can be implemented as a lookup table with 2^m words of *n* bits each. Fixed tables are normally used, as in the Data Encryption Standard (DES), but in some ciphers the tables are generated dynamically from the key (e.g. the Blowfish and the Two fish encryption algorithms).

Q2. Distinguish between Differential and Linear Cryptanalysis techniques. Explain their features with design characteristics along with diagram. (10)

Answer:

Linear Cryptanalysis:

Linear cryptanalysis is a known plaintext attack, in which the attacker studies probabilistic linear relations known as linear approximations between parity bits of the plaintext, the Ciphertext and the secrete key.

Linear cryptanalysis was first discovered by Matsui and Yamagishi in 1992. Linear cryptanalysis focuses on statistical analysis against one round of decrypted cipher text. In linear cryptanalysis, the role of the attacker is to identify the linear relation between some bits of the plaintext, some bits of the ciphertext and some bits of the unknown key. In linear cryptanalysis, the cryptanalyst decrypts each cipher using all possible sub keys for one round of encryption and studies the resulting intermediate cipher text to analyze the random results.

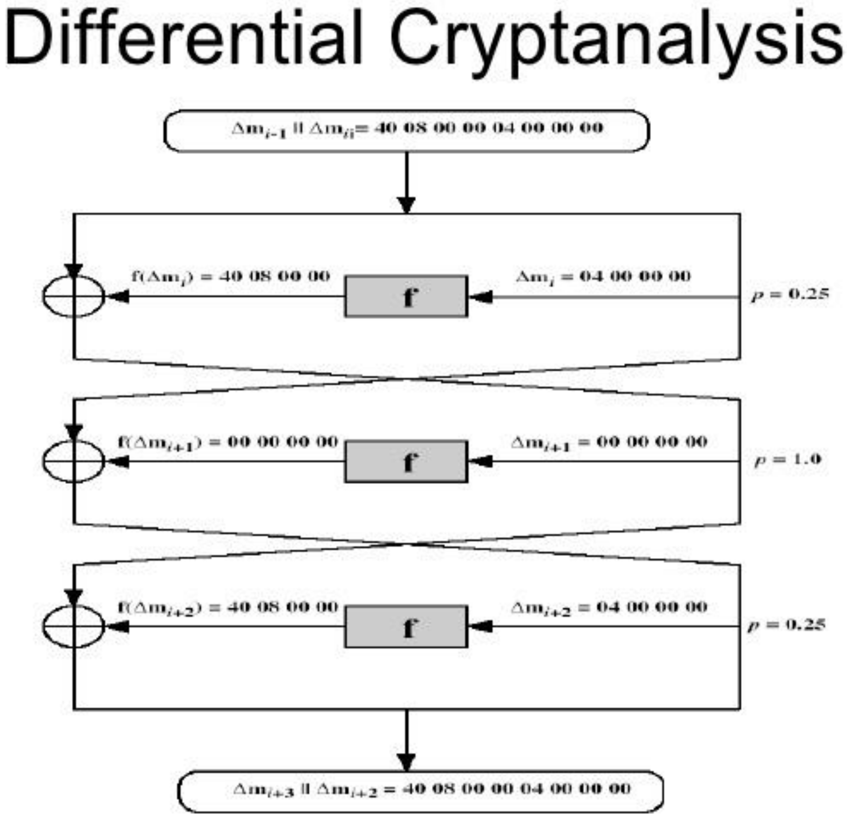
Differential Cryptanalysis

Differential cryptanalysis can be described as a general form of cryptanalysis that is primarily applicable to block ciphers, cryptographic hash functions. It entails a careful analysis of how differences in information input can affect the resulting difference at the output.

Differential analysis was discovered by Israeli researchers Eli Biham and Adi Shamir.

Differential analysis focuses on statistical analysis of two inputs and two outputs of a cryptographic algorithm. Differential analysis focuses on statistical analysis of two inputs and two outputs of a cryptographic algorithm. In differential cryptanalysis, the role of the attacker is to analyze the changes in some chosen plaintexts and the difference in the outputs resulting from encrypting each one, it is possible to recover some of the key.

In differential cryptanalysis, the changes to the intermediate cipher text are obtained between multiple rounds of encryption. The attacks can be combined, and this can be referred to as differential-linear cryptanalysis.


Differential Cryptanalysis
$\Delta m_{i-1} \| \Delta m_{i}$= 40 08 00 00 04 00 00 00
$f(\Delta m_i)$ = 40 08 00 00
f
Δm_i = 04 00 00 00
$p = 0.25$
$f(\Delta m_{i+1})$ = 00 00 00 00
f
Δm_{i+1} = 00 00 00 00
$p = 1.0$
$f(\Delta m_{i+2})$ = 40 08 00 00
f
Δm_{i+2} = 04 00 00 00
$p = 0.25$
$\Delta m_{i+3} \| \Delta m_{i+2}$ = 40 08 00 00 04 00 00 00

Features with design characteristics of Linear Cryptanalysis

Differential cryptanalysis can be described as a general form of cryptanalysis that is primarily applicable to block ciphers, cryptographic hash functions. In other words, it entails a careful analysis of how differences in information input can affect the resulting difference at the output.

In block cipher, differential analysis can be described as a set of techniques for tracing differences through the network of transformation, discovering where the cipher exhibits what is known as non-random behavior and exploiting such details to recover the secrete key (cryptography key).

For any particular cipher, the input difference must be keenly selected for the attack to be successful. An analysis of the algorithm's internals is undertaken; the standard method is to trace a path of highly probable differences through the various stages of encryption, referred to as *differential characteristic*. In the process, observing the desired output difference between the two chosen or unknown plaintext inputs suggests possible key values.

Difference Between Linear and Differential Cryptanalysis

In cryptography, **Linear cryptanalysis** is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. Attacks have been developed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used attacks on block ciphers; the other being differential cryptanalysis.

Q3. Apply the following 3 codes to the given text:

Monoalphabetic Cipher

Playfair Cipher

Vigenere Cipher

Step by step process should be mentioned when performing the activity.

Answer: Monoalphabetic Cipher

Code conversion apply monoalphabetic Cipher to the following text

(i) **Plain text for Monoalphabetic Cipher**:

The sections on quantum cryptography, quantum proper ties of squeezed light, and experimental efforts to measure gravitational waves provide adequate introduction to these exciting applications of quantum optics.

Step by step encryption

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.

Step1: we will encrypt T to G, H to S, E to V so on in the whole text

Result after encryption at sending side: GSV HVXGRLMH LM JFZMGFN XIBKGLTIZKSB, JFZMGFN KILKVI GRVH LU HJFVVAVW ORTSG, ZMW VCKVIRNVMGZO VUULIGH GL NVZHFIV TIZERGZGRLMZO DZEVH

KILERWV ZWVJFZGV RMGILWFXGRLM GL GSVHV VCXRGRMT ZKKORXZGRLMH LU JFZMGFN LKGRXH.

For Decryption we will reverse this the above process

The above plain text will decrypt to the original text at the receiving end

Result After Decryption at receiving end: -

The sections on quantum cryptography, quantum proper ties of squeezed light, and experimental efforts to measure gravitational waves provide adequate introduction to these exciting applications of quantum optics.

(ii) Playfair cipher or Playfair square or Wheatstone-Playfair cipher is a manual symmetric encryption technique and was the first literal diagram substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair for promoting its use.

Below an example you can find the calculator for encryption and decryption to play with. It uses most common rules for Playfair cipher:

1. 'J' is replaced with 'I' to fit 5x5 square
2. 'X' is used as substitution in case you need to fill second letter in the diagram, or split two identical letters
3. Playfair square is filled row-by-row, starting with the keyword.

Plain Text for Encryption: “The implementation of a public key cryptography package needs to ensure that the random number object used in the generation of key pairs cannot be accessed by clients of the package.”

Step1: Playfair square

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

Step 2:

Result After Encryption:

SBHVNKEOOCKFGFVPOPDFMZETRHOBCMYCKSKVAVZPSMRDNGVBOD
HETYXOPFRYBLDILQSBCVFWENNORUCHVMHGHDYQLHHAKFBHVBOD
AVSGPONLOBSMVGIYDROWOPBKDVEUDHLZLHECCMSVDOYTNLSBHO
RDNGVB

III): Vigenere Cipher

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the *Vigenère square or Vigenere table*.

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Step1: input Plane text for encryption:

> “Components for these systems are now commercially available, and it seems very likely that quantum cryptography will be an important technology long before quantum computers of useful size are constructed.”

Encryption

The plaintext(P) and key(K) are added modulo 26.

$E_i = (P_i + K_i) \bmod 26$

Decryption

$D_i = (E_i - K_i + 26) \bmod 26$

Step2: Keyword: AYUSH

Output: Ciphertext: GCYCZFMLYLEIM

For generating key, the given keyword is repeated in a circular manner until it matches the length of the plain text.

The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"

The plain text is then encrypted using the process explained below.

```
string cipherText(string str, string key)
{
    string cipher_text;

    for (int i = 0; i < str.size(); i++)
    {
        // converting in range 0-25
        char x = (str[i] + key[i]) %26;

        // convert into alphabets(ASCII)
        x += 'A';

        cipher_text.push_back(x);
    }
    return cipher_text;
}

// This function decrypts the encrypted text
// and returns the original text
string originalText(string cipher_text, string key)
{
    string orig_text;

    for (int i = 0 ; i < cipher_text.size(); i++)
    {
        // converting in range 0-25
        char x = (cipher_text[i] - key[i] + 26) %26;

        // convert into alphabets(ASCII)
        x += 'A';
        orig_text.push_back(x);
    }
    return orig_text;
}
```

Step 3

Out Result After Encryption: Efkehvmpkq uhz bjvqt lgavvkh tzm pfu rhuugiaxttta rtpbtidcc, pgl qv jctfa dgiw absmnp rwtb ywrlinu ktpnihozcgfn pqtn sc pg qurfpitvb vvawgwtqxw ahvo dvddkm ywrlinu kqdnjmmzu fd jlmnwc qxsm itv adgabtlaixl

The above second function apply to out put result of Encryption will the qive the decrypted text at the receiving end

Out Result After decryption:

> “Components for these systems are now commercially available, and it seems very likely that quantum cryptography will be an important technology long before quantum computers of useful size are constructed.”