FAIZ HAMMAD
2K17/MC/041

Assignment-2

Cryptography and Network security

Ques 1.

Ans:- (1) →

(a)

BLOCK CIPHER

1) Block cipher converts the plain text into cipher text by taking plain text's block at a time

2) Block cipher uses either 64 bits or more than 64 bits

3) The complexity of block cipher is simple

4) It uses ~~more~~ confusion as well as diffusion

5) reverse encrypted text is hard

6.) The algorithm modes which are used are: ECB and CBC

7.) ~~It~~ slow.

8.) It works on transposition techniques like Caeser cipher, polygram substitution etc.

STREAM CYPHER.

1) Stream cipher converts the plain text into cipher text taking 1 byte of plain text at a time.

2) While stream cipher uses 8 bits

4) It uses or is more complex.

4) It uses only confusion.

5) reverse encrypted text is easy.

6.) The algorithm modes which are used are ~~E~~ CFB and OFB

7) It is faster.

8) It works on substitution techniques like rail-fence technique etc.

(b)

CONFUSION	DIFFUSION
1) It is a cryptographic technique which is used to create faint cipher texts.	1) It is used to create cryptic plain texts.
2) This technique is possible through Substitution algorithm	2) It is possible through transportation algorithm
3) In confusion, if one bit within the secret's modified most of all bits within the cipher text all bits within the cipher text also will be modified	3) 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.	4) redundancy is increased in resultant.

Ques 2.

Ans:- (2) →

With given n bits, There are 2^n possible different plaintext blocks and, for the encryption to be reversible, each must produce a unique ciphertext block. Such a transformation is called reversible or non-singular. The If we limit ourselves to reversible mappings, the number of different transformations is $2^n!$.

Explanation: For a n-bit block size are 2n possible different plaintext blocks and 2n possible different ciphertext blocks. For both the plaintext and ciphertext, if we treat the blocks and unsigned integer, the values are in the range 0 through 2n-1. For a mapping to be reverse, each plaintext block must map

into a unique ciphertext block. Thus, to enumerate all possible reversible mappings, the block will value 0 can map into anyone of 2n possible ciphertext blocks. For given mapping of the block with value 0, the block with value 1 can map into any one of 2n-1 possible ciphertext blocks, and so on. Thus, the total number of reversible mappings is $(2^n)!$

Ques 3.

Ans:- (3) →

A block cipher is designed by considering its three critical aspects which are the follwing:

(1) NUMBER OF ROUNDS

The number of rounds judges the strength of the block cipher algorithm. It is considered that more is the number of rounds, difficult is for cryptanalysis to break the algorithm. It is considered that even if the function F is relatively weak, the number of rounds would make the algorithms tough to break.

(2) DESIGN OF FUNCTION F

The function F of the block cipher must be designed such that it must be impossible for any cryptoanalysis to unscramble the substitution. The criterion that strengthens the function F is it non-linearly.

More is the function F is nonlinear, more it would be difficult to crack it. Well, while designing the function F it should be confirmed that it has a good avalanche propisty which states that a change in one bit of input must reflect the change in many bits of output.

(3.) KEY SCHEDULE ALGORITHM

It is suggested that the key schedule should confirm the strict avalanche effect and bit independence criterion.

Ques 4.

Ans:- (4) → AVALANCHE EFFECT IN DES

- A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext.
- In particular, a change in one ~~bit~~ bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext.
- This is referred to as the avalanche effect. If the change were small, this might provide a way to reduce the size of the plaintext or key space to be searched.

Ques 5.

Ans:- (5) →

We need only to determine the probability that for the remaining $N-t$ plaintext P_i,

We have,

$$E[K, P_i] \neq E[K', P_i].$$

But,

$E[K, P_i] = E[K', P_i]$ for all remaining P_i, with probability, $1 - \frac{1}{(N-t)!}$

Ques 6.

Ans :- (6) →

Listing all 1-bit possibilities

A	B	$A \oplus B$	$(A \oplus B)'$	$A' \oplus B$
0	0	0	1	1
0	1	1	0	0
1	0	1	0	0
1	1	0	1	1

We also need the equality $A \oplus B = A' \oplus B'$, which can be easily seen. Now considering two XOR operations. If the plaintext and key for an encryption are complemented, then the inputs to the first XOR are also complemented. The output then is the same as for the uncomplemented inputs. Further down, we see that only one of the two inputs to the second XOR is complemented, therefore, the output is the complement of the output that would be generated by uncomplemented inputs.

Ques 7.

Ans :- (7) → The result can be demonstrated by tracing through the way in which the bits are used. An easy, but not necessary, way to see this is to number the 64 bits of the key as follows:

2113355-1025554-0214434-1123334-0012343-2021453-0202435-0110414
-1031925-1176107-2423401-7632789-7632789-7452553-0858846-6836042-
9495226-

The first bit of the key is identified as 21, the second as 10, the third as 13 and so, on the eight bits that are not used in the calculation are unnumbered. The numbers 01 through 28 and 30 through 57 are used.

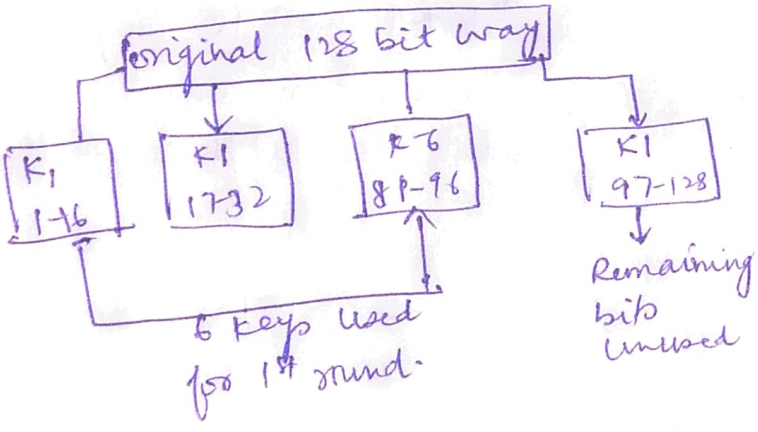
The reason for this assignment is to clarify the way in which the subkeys are chosen. With this assignment, the subkey for the first iteration contains 48 bits, 01 through 24 and 30 through 53, in their natural numerical order. It is easy at this point to see that the first 24 bits of each subkey will always be from the bits designated 01 through 28 and the second 24 bits of each subkey will always be from the bits designated 30 through 57.

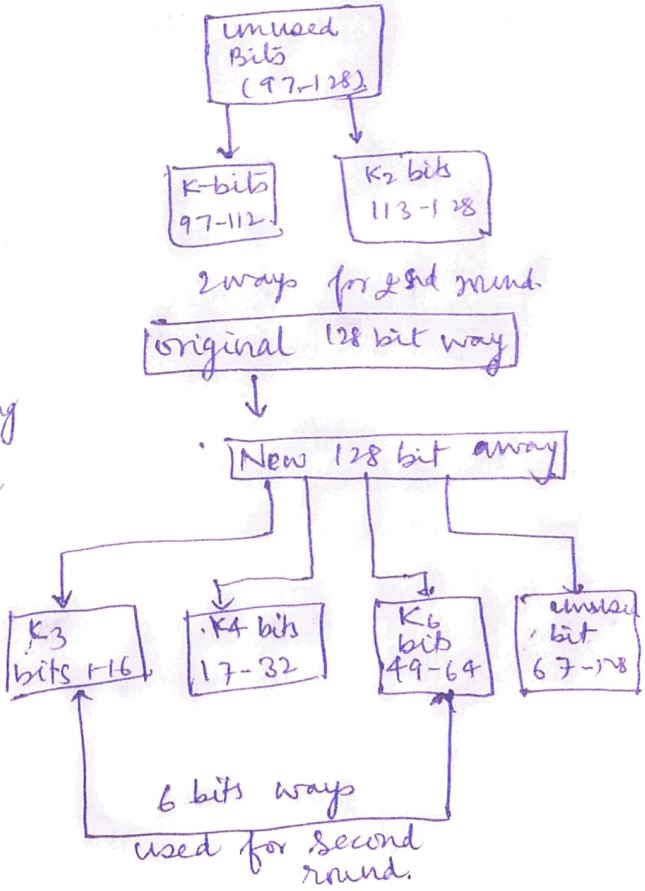
Ques.

Ans:-(8) →

(a) STEPS INVOLVED IN ONE ROUND OF IDEA

- There are 8 rounds in IDEA.
- Every single requires a number of operations around the four data blocks applying 6 steps
- These steps work numerous mathematical activities
- There are multiple *, add *. & XOR operations
- Multiplying * means multiplication modules.
- Add * requires addition modules.





Steps involved in one round of IDEA.

1.) $P_1 \oplus K_1$

2) $P_2 \oplus K_2$

3) $P_3 \oplus K_3$

4) $P_4 \oplus K_4$

5) (1) ⊕ (3)

6) (2) ⊕ (4)

7) (5) ⊕ K_6

8) (6) ⊕ (7)

9) (8) ⊙ K_6

10) 7 ⊞ 9

11) (1) ⊕ (9)

12) (3) ⊕ (9)

13) (2) ⊕ (10)

14) (4) ⊕ (10)

(6) OUTPUT TRANSFORMATION

- It can be one time procedure
- It requires places by the end of the 8th round
- The input towards the output transformation is, a 64 bit value divided into 4 subblocks
- The 4 16-bit subway (K_1 to K_4) are used here.
- The process of the outcome transformation can be follows:

Step 1: Multiply * R_1 and K_1

↓

Step 2: Add * R_2 and K_2

↓

Step 3: Add * R_3 and K_3

↓

Step 4: Multiply * R_4 and K_4

C) STRENGTH OF IDEA.

- It uses 128 bit key double than the key size of DES.
- Size of the keyspace ~~(2^{128})~~ (2^{128})
- Examining half of the possible key using a single computer take more than 54×10^{23} years