TC Assignment 1

Name -
Roll No -

23^{rd} January 2025
Total Marks - 10

---

1. Define Known Plaintext Attack [2]

2. If we have a block cipher which takes a key of size 64 bits. Consider that we have by some technique able to obtain 6 key bits in time $O(1)$, then what is the complexity of exhaustively searching the full key? [0.5]

   - Since 6 bits were already rcovered, the xhaustive search would be - $2^{64-6} = 2^{58}$

3. The success of an attack is measured in three quantities, what are those? [1]

   - Time, memory and data

4. Consider that you have a block cipher with key size, k = 48-bits and block size (i.e. the size of plaintext and ciphertext) of, n = 32-bits. Then what is the minimum number of plaintext-ciphertext pairs required to exhaustively search for the correct key with probability 1. [1]

   - For a key size k and block size n, the number of pairs required is $\lceil \frac{k}{n} \rceil$, so in this case it would be $\lceil \frac{48}{32} \rceil = 2$

5. For a block cipher with key size k, an attack will be said to be non-generic if [0.5]

   (a) $D < 2^k$
   (b) $D \leq 2^k$
   (c) $D \geq 2^k$
   (d) $D = 2^k$

   - here all T,M,D $< 2^k$

6. If a function $F : \{0,1\}^6 \rightarrow \{0,1\}^6$ is defined as $F(x,t) = x \oplus t$, for all x and a fixed t, then show with an example that

$$Pr[\Delta x \xrightarrow{F} \Delta x] = 1$$

   [2]

   - Any answer on the lines of the following will be accepted:
     Consider two inputs a and a' then we have

$$b = F(a) = a \oplus t, \quad b' = F(a') = a' \oplus t$$

     . So the input difference $\Delta(x) = a \oplus a'$ and the output difference is $\Delta(y) = a \oplus t \oplus a' \oplus t = a \oplus a' = \Delta(x)$.

     Thus we have $Pr[\Delta x \xrightarrow{F} \Delta x] = 1$

7. What will be the best complexities in terms of (T, M, D) while implementing a TMTO attack on AES-128? [1]

   - For AES-N, the key size is $N = 128, 192, 256$ and so the complexities would be $T = M = 2^{64}/2^{96}/2^{128}$ and $D = O(1)$

8. Consider the following DDT table of the Sbox S - $[7, 6, 0, 4, 2, 5, 1, 3]$

   Answer the following questions

8	0	0	0	0	0	0	0
0	2	2	0	2	0	0	2
0	0	2	2	0	0	2	2
0	2	0	2	2	0	2	0
0	2	0	2	0	2	0	2
0	0	2	2	2	2	0	0
0	2	2	0	0	2	2	0
0	0	0	0	2	2	2	2

(a) What is the value of probability $Pr[\Delta x = 3 \xrightarrow{S} \Delta y = 3]$? [0.5]

(b) What is the value of probability $Pr[\Delta x = 6 \xrightarrow{S} \Delta y = 7]$? [0.5]

(c) What is the maximum value the probability $Pr[\Delta x \xrightarrow{S} \Delta y]$ can have, for any input difference Δx and any output difference Δy? [1]