PAST PAPER WITH SOLUTION

Question 1: Give short (one-line) explanation for each of the following: **[10 points]**

a) Brute-force attack

Exhaustive key search

b) Confusion

Complex relation between key and plaintext/ciphertext. Hard to deduce key from plaintext/ciphertext pair

c) Diffusion

Complex relation between plaintext and ciphertext. Hard to deduce bits of plaintext from ciphertext

d) Key space for Vigenre cipher with a known key length of n

26^n

e) Key space for a mono-alphabetic substitution cipher with k letters

K!

Question 2: The following cipher is encrypted using well know shift cipher. Decipher the text and find out the mapping of the alphabets. **[10 points]**

Wkqqsurkylryyucevtrky

Shift Alphabet is K

Maggi khao bhook suljhao

Question 3: What is the difference between one-time pads and Stream ciphers? Give an example showing how Stream Ciphers are vulnerable against reuse of cipher key. **[5 points]**

One-time pad: Random Keys
Stream Ciphers: Pseudo-Random Keys using PRG

Never use stream cipher key more than once !!

$$C_1 \leftarrow m_1 \oplus PRG(k)$$
$$C_2 \leftarrow m_2 \oplus PRG(k)$$

Eavesdropper does:

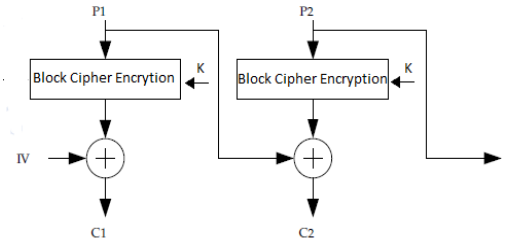
$$C_1 \oplus C_2 \rightarrow m_1 \oplus m_2$$

Enough redundancy in English and ASCII encoding that:

$$m_1 \oplus m_2 \rightarrow m_1 , m_2$$

Question 4: PBC (Plain Block Chaining) is a new block cipher mode that adds the plaintext message P_i to the encrypted message C_i as depicted in the following diagram: **[10 points]**

a) Write down the encryption and decryption function for PBC (Plain Block Chaining).
b) How many text blocks are false if one of the transmitted blocks is corrupted?



Encryption: Ci = Ek (Pi) ⊕ Pi-1, P0 = IV
Decryption: Pi = Dk(Ci⊕ Pi-1), P0 = IV

All the subsequent blocks will decrypt incorrectly if there is a corrupt block or one block is lost.

Question 5: Consider the Mix-Columns transformation of AES algorithm. Find out the resultant state matrix by applying this transformationon the following matrices: **[5 points]**

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

$$
\begin{aligned}
(\{02\}\cdot\{87\}) \oplus (\{03\}\cdot\{6E\}) \oplus \{46\} \oplus \{A6\} &= \{47\}\\
\{87\} \oplus (\{02\}\cdot\{6E\}) \oplus (\{03\}\cdot\{46\}) \oplus \{A6\} &= \{37\}\\
\{87\} \oplus \{6E\} \oplus (\{02\}\cdot\{46\}) \oplus (\{03\}\cdot\{A6\}) &= \{94\}\\
(\{03\}\cdot\{87\}) \oplus \{6E\} \oplus \{46\} \oplus (\{02\}\cdot\{A6\}) &= \{ED\}
\end{aligned}
$$

For the first equation, we have $\{02\}\cdot\{87\} = (0000\ 1110) \oplus (0001\ 1011) = (0001\ 0101)$ and $\{03\}\cdot\{6E\} = \{6E\} \oplus (\{02\}\cdot\{6E\}) = (0110\ 1110) \oplus (1101\ 1100) = (1011\ 0010)$. Then,

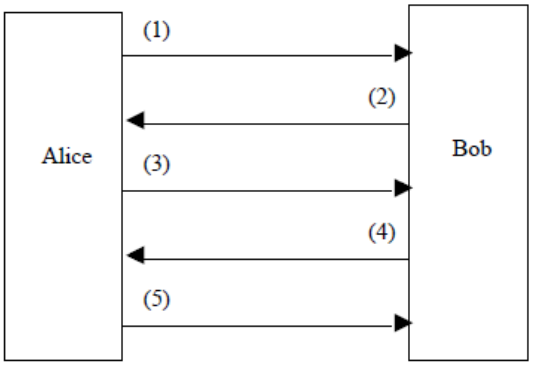
$$
\begin{aligned}
\{02\}\cdot\{87\} &= 0001\ 0101\\
\{03\}\cdot\{6E\} &= 1011\ 0010\\
\{46\} &= 0100\ 0110\\
\{A6\} &= \underline{1010\ 0110}\\
&\quad 0100\ 0111 = \{47\}
\end{aligned}
$$

The other equations can be similarly verified.

Resultant Matrix

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

Question 6: Suppose Alice and Bob have pre-shared secret key $K_{AB.}$ Design a protocol that can help Alice and Bob authenticate the originality of messages of each other on the basis of the shared secret key K_{AB}



.
[10 points]

Let k = K_{AB}.
Protocol :

1. **Alice sends a communication request to Bob**

2. **Bob sends a random number R1**
3. **Alice sends Ek(R1) and a random number R2**
4. **Bob sends Ek(R2) and the string „I trust you“, if he was able to decrypt Ek(R1). Otherwise, he sends the string „No“.**
5. **Alice sends the string ,,I trust you, too“ , if Alice was able do decrypt Ek(R2). Otherwise, she sends the string ,,No“.**

Step 4) represents the first check, namely the check of Alice. If the check fails the communication is aborted. In step 5) Alice checks Bob. If the check fails the communication is aborted. If the check is successful the communication can start. The protocol is safe against passive attacks, because an attacker listening to the communication does not retrieve any information, which could be used for later authentication attempts (although the collected information can be used to attack the encryption itself). However, the protocol does not protect Alice and Bob against active man-in-the-middle attacks, during which an attacker acts as an intermediate between Alice and Bob intercepting and modifying the messages exchanged.

Question 7: Construct a secure MAC with following two optimizations. **[10 points]**

a) No final encryption step is required for protection against existential forgery.
b) No dummy block is required to resolve ambiguity problem due to invertible padding scheme.

CMAC