UBUA VERA

16/SCI01/048

COMPUTER SCIENCE

1. Write short note on the following:
2. **Chosen-ciphertext attack-** this is an attack model for cryptanalysis where the cryptanalyst can gather information by obtaining the decryptions of chosen ciphertexts. From these pieces of information, the adversary can attempt to recover the hidden secret key used for decryption.
3. **Chosen – key attack-** this is an attack model against symmetric ciphers, whereby an attacker who knows the key can find a structural property in cipher, where the transformation from plaintext to ciphertext is not random. There is no common formal definition for what such a transformation may be.
4. **Rubber – hose cryptanalysis-** is a euphemism for the extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by coercion or torture[—such as beating that person with a rubber hose, hence the name—in contrast to a mathematical or technical cryptanalytic attack.
5. There is no code that cannot be broken and there is no algorithm that is secured, justify.
6. Write short note on Brute-force attack.

A brute force attack is an attempt to crack a password or username or find a hidden web page, or find the key used to encrypt a message, using a trial and error approach and hoping, eventually, to guess correctly. This is an old attack method, but it's still effective and popular with hackers.

Depending on the length and complexity of the password, cracking it can take anywhere from a few seconds to many years. In fact, IBM reports that some hackers target the same systems every day for months and sometimes even years.

1. Given the following plaintext, encrypt it using Caesar cipher. Plaintext: corona virus is killing around the world

**dpspob wjsvt jt ljmmjoh bspvoe uif xpsme**

1. Decipher the following ciphertext, given C = E(7,p) = p+7 mod26. JYFWAVWYHWOF PZ UVA AVV KPMMPJBSA

JYFWAVWYHWOF- **CRYPTOPRAPHY**

PZ- **IS**
UVA- **NOT**

AVV- **TOO**

KPMMPJBSA- **DIFFICULT**

1. Given the following plaintext and the ciphertext, 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 M O R S A T V E Y Z P N X D G U B L W C Q J F H K I
2. What type of cipher is this?
3. Decipher the following ciphertext: RMD KGQ OA XK TLYADS.
4. Encrypt the following plaintext: I JUST CANNOT BREAK YOUR CODE
5. Write short note on play-fair cipher

The Playfair cipher is a digraph substitution cipher. It employs a table where one letter of the alphabet is omitted, and the letters are arranged in a 5x5 grid. Typically, the J is removed from the alphabet and an I takes its place in the text that is to be encoded. To encode a message, one breaks it into two-letter chunks. Repeated letters in the same chunk are usually separated by an X. The message, "HELLO ONE AND ALL" would become "HE LX LO ON EA ND AL LX". Since there was not an even number of letters in the message, it was padded with a spare X. Next, you take your letter pairs and look at their positions in the grid.

1. Using the play-fair technique encrypt the following plaintext given HORIZONTAL as the key: SIMPLE SUBSTITUTION H O R I/J Z N T A L B C D E F G K M P Q S U V W X Y
2. Using the play-fair technique encrypt the following plaintext given RECEIVER as the key: SIMPLE SUBSTITUTION R E C I V A B D F G H K L M N O P Q S T U W X Y Z
3. In vigenere cipher, encrypt this given plaintext: “keep it secret” using “unbreakable” as the key.

Plaintext- KEEPITSECRET

Key- UNBREAKABLE

Keystream- UNBREAKABLEU

Cipher Text- **ERFGMTCEDCIN**