ADEYEMI TESLIMAT ADEBUNMI

16/SCI01/003

CSC 418 ASSIGNMENT

1. Write short notes on the following

Chosen-ciphertext attack: A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key. When a cryptosystem is susceptible to chosen-ciphertext attack, implementers must be careful to avoid situations in which an attackers might be able to decrypt chosen ciphertexts (i.e., avoid providing a decryption scheme).

Chosen – key attack: A chosen-ciphertext attack 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. For formal definitions of security against chosen-ciphertext attacks, Chosen-key attacks are a bit different than other kinds of cryptographic attacks. Usually, they are intended to not just break a cipher but to break the larger system which relies on that cipher. The attacker should have some knowledge regarding the relationship between various keys that can be used in the cipher.

Rubber – hose cryptanalysis: In cryptography, rubber-hose cryptanalysis is the extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by coercion or torture, in contrast to a mathematical or technical cryptanalytic attack. The euphemistic term refers to beating someone with a rubber hose until they cooperate. 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.

1.
2. 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. A brute force attack, also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered. The longer the password, the more combinations that will need to be tested. a **brute-force attack** consists of an attacker submitting many [passwords](https://en.wikipedia.org/wiki/Password) or [passphrases](https://en.wikipedia.org/wiki/Passphrase) with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the [key](https://en.wikipedia.org/wiki/Key_%28cryptography%29) which is typically created from the password using a [key derivation function](https://en.wikipedia.org/wiki/Key_derivation_function). This is known as an **exhaustive key search**. A brute-force attack is a [cryptanalytic attack](https://en.wikipedia.org/wiki/Cryptanalytic_attack) that can, in theory, be used to attempt to decrypt any encrypted data[[1]](https://en.wikipedia.org/wiki/Brute-force_attack#cite_note-FOOTNOTEPaar20107-1) (except for data encrypted in an [information-theoretically secure](https://en.wikipedia.org/wiki/Information-theoretically_secure) manner). Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier.
3. 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**