**KEYWORDS** A

* Encrypted message – a message which has gone through the process of converting information or data into a code to prevent unauthorized access.
* Decrypted message – a message which has gone through the process of converting previously encrypted data into information that can be read by humans and/or computers
* Coordinates - each of a group of numbers used to indicate the position of a point, line, or plane.
  + Latitude - the angular distance of a place north or south of the earth's equator, usually expressed in degrees and minutes.
  + Longitude - the angular distance of a place east or west of the Greenwich meridian, usually expressed in degrees and minutes.
* Scientific demonstration - a procedure carried out for the purposes of demonstrating scientific principles, rather than for hypothesis testing or knowledge gathering
* ASCII Message - ASCII (American Standard Code for Information Interchange) is the most common character encoding format for text data in computers and on the internet.
* Decipher - convert an encrypted message into normal language to succeed in understanding, interpreting, or identifying the message.

**CRYPTOGRAPHY** A

*Some Keywords:*

* Algorithm: a precise set of instructions that tells programs how to scramble and unscramble data.
* Strong Crypto: good algorithms
* Weak Crypto: bad algorithms
* Encrypt: Scrambling data to make it unrecognizable
* Decrypt: Unscrambling data to its original format
* Cipher: Another word for algorithm
* Key: A complex sequence of alpha-numeric characters, produced by the algorithm, that allows you to scramble and unscramble data
* Plaintext: Decrypted or unencrypted data (it doesn’t have to be text only)
* Ciphertext: Data that has been encrypted
* Brute force: a trial and error method of trying every possible combination of characters against the encrypted data in an attempt to discover the key
* Cryptosystems: the combination of three elements –
  + the encryption engine - part of the software that starts the encryption with the selected algorithm
  + keying information - portion of the software that creates (and sometimes manages) the keys needed to encrypt and decrypt data
  + operational procedures – explains how all of these parts interact and how the output, or result, is formatted and what file extension (if any) is used
* Random Number Generator - something that takes input from an entropic event and converts it to a number
* Pseudo Random Number Generator - generates random numbers, but it generates the same random numbers every time you run it.

*Types of Ciphers:*

* Concealment ciphers - hide a message in plainsight. Eg -
  + Taylor Swift’s song “thanK you aIMee” or
  + Dear Mr Wickam, ta**h**nk you, th**e** money is received. Th**y** are praised.
* Substitution ciphers - substitute one letter or character for another. Eg –



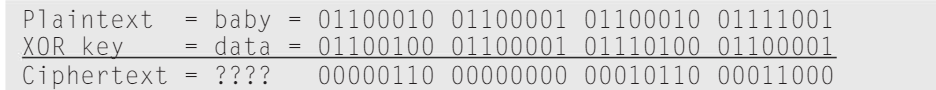
* + Message – HI THERE
  + Cipher text – ZA LZWJW
  + Key – 18 shifts
* Transposition ciphers - This type of cipher changes the order of the letters of the original message. Eg –
  + The German Enigma cipher
  + Encrypted message – MME YER NII ASC
  + Message – My name is Eric

M Y N A

M E I S

E R I C

* XOR (not recommended – easy to break) – Exclusive-or



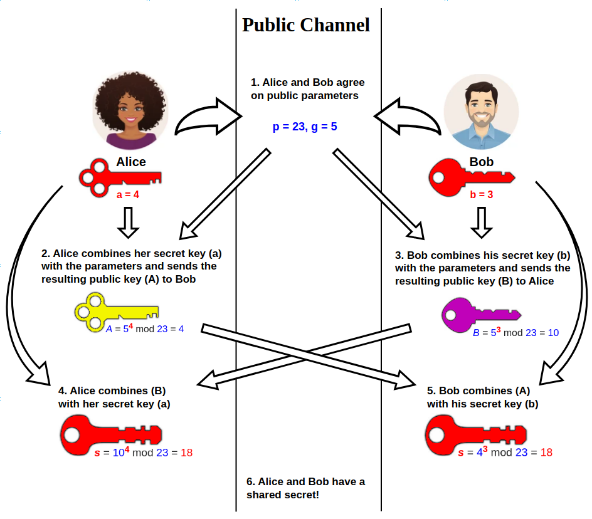
* + ASCII is a table that assigns a keyboard character to the numbers 0 to 256
  + Cipher text - ^F^@^V^Z
  + If you again XOR the ciphertext with the XOR key, you’ll get the plain text

*Symmetric Keys*

* Symmetric algorithms all use one key to encrypt data and the same key to decrypt it.
* When the user of a symmetric algorithm creates a key, most symmetric algorithms create a key table from the original key. This is also known as the key setup or initialization.
* Keys in the key table are longer than the original key.
* To make the PRNG better, the PRNG takes some sort of other random input from your computer and mixes that up with the pseudo-random number from the PRNG to create another number.
* Block ciphers take exact chunks of data, encrypt them with the key table, and then take the next chunk, and so on.
  + If two different chunks of data contain the exact same data, the ciphertext could be exactly the same.
* Stream ciphers are very simple to program and they process very quickly. Eg – RC4 in SSL (Secure Sockets Layer)
* DES stands for Digital Encryption Standard.
  + DES is a block cipher that uses a 56-bit key to create the key table.
  + Then it goes through the process of combining a key from the key table with the block of plaintext.
  + After the key and the plaintext have been combined, DES goes through 16 more changes (called rounds) to thoroughly mix up the ciphertext.
  + To decrypt the data, DES just goes through all the changes in reverse order.
* Triple DES does something three times more than normal DES.
  + Triple DES encrypts the plaintext with the first key, encrypts that ciphertext with another 56-bit key, and then encrypts the ciphertext with another 56-bit key
* IDEA stands for International Data Encryption Algorithm
  + This algorithm starts out with a 128-bit key.
  + It then breaks up the 128-bit key into a total of 56 subkeys
  + Then the bits of the original 128-bit key are shifted 25 bits to the left
* AES stands for Advanced Encryption Standard

*Asymmetric Keys*

* Asymmetric keys make two separate keys that are mathematically connected.
* There is a “private” key that is never revealed to anyone to decrypt the data received
* The recipient uses their corresponding “public” key that everyone can have to encrypt the data.
* RSA uses prime numbers to create each of the keys (private & public), but using those keys to encrypt a large amount of data is impractical due to the amount of time it takes a computer to process the encryption.
* An encryption program that uses RSA encrypts the data with a symmetric algorithm such as RC4 (or DES, or IDEA, and so on).
* Then the symmetric key created by RC4 is encrypted with the recipient’s public key.
* When the recipient gets the message, she uses her private key to decrypt the RC4 key, and when the RC4 key is decrypted, the bulk of the message can be decrypted.
* Diffie-Hellman (DH) is not an encryption algorithm; rather, it is a key exchange algorithm.



* PGP (Pretty Good Privacy) is an encryption program that uses both symmetric and asymmetric algorithms to encrypt data.
* PGP is a hybrid cryptosystem.
* When a user encrypts plaintext with PGP, PGP first compresses the plaintext.
* Then it creates a session key, which is a one-time-only secret key. This session key encrypts the data.
* When the data is encrypted, the session key is then encrypted to the recipient’s public key.
* This public key-encrypted session key is transmitted along with the cipher-text to the recipient.

