COURSE OUTLINE

This course will be defended into 3 modules:

MODULE 1: CRYPTOGRAPHIC TECHNIQUES TERMS AND CONCEPTS:

* Plaintext And Cipher Text, Substitution Techniques, Transposition Techniques, Encryption and Decryption, Symmetric and Asymmetric Key Cryptography, Steganography, Key Range and Key sizes .

MODULE 2: COMPUTER BASED SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS:

* Algorithm types and modes, Symmetric cryptography such as DES and AES.

MODULE 3: COMPUTER BASED ASYMMETRIC KEY CRYPTOGRAPHY:

* A brief history of assymetric key cryptography, an overview, the RSA algorithm

BASIC CONCEPTS

1. Cryptography: This is the science of encompassing the principle and methods of transforming an intelligible message into one that is unintelligible or intelligible by the sender, and there will be transforming that message back to its original form by the receiver. It deploys the use of mathematical and logical reasoning of the tools.
2. Plaintext: The original intelligible message is called the plaintext
3. Cipher-text: It is the transformed message.
4. A cipher: is the algorithm to transforming an intelligible message into one that is not intelligible by transposition and/or substitution
5. Key: Some critical information used by the cipher known only to the sender and receiver.
6. Encipher (Encryption): This is the process of converting plaintext to cipher-text using a cipher and a key.
7. Decipher (Decryption): This is the process of converting cipher-text to plaintext using a cipher and a key.
8. Crypt Analysis: This is the study of principles and methods of transforming an unintelligible message back to its original state without prior knowledge of the key.
9. Cryptology: Both Cryptography and crypt analysis fall under this category.

Cryptographic System are generally classified along 3 independent dimensions:

1. Types Of Operations Used For Transforming Plaintext To Cipher-Text:

All the encryption algorithm are usually based on 2 general principles;

* + Substitution (The elements within the plaintext are mapped to different elements which must not necessarily be in the plain text).

E.g. I love you: x uktz uvy

* + Transposition (The elements within the plaintext are just rearrange)

E.g. I love you: vloe i oyu

1. If the sender and receiver use the same key. It is said to be a symmetric key or a single key or conventional encryption. On the other hand, if the sender and the receive use different keys, then it is said to be asymmetric key or public key encryption.
2. The way in which the plaintext is process:
3. Block Cipher: This takes the input as a block unit, performs some operation on this block and produces and output block per each input block.
4. Stream Cipher: This process the input elements continuously producing ouput elements one at a time.
5. Steganography: This refers to the arts or science of hiding a message within another message, text or image. *The method of steganography conceals the existence of the message whereas the methods of cryptography renders the message unintelligible by applying certain transformations on the text.*

E.g.

1. The sequence of first letters of each word of the overall message spells out the real hidden message
2. Subset of the words of the overall- message is convey the hidden message

Various Other Techniques have been used historically,some of them are character making, selected letters of printed or typewritten text are overwritten in pencil.

* + - The marks are ordinarily not visible unless the paper is held too an angle to bright light.
    - Invisible ink: A number of substances can be used for writing but leaving no visible trace until heat or some chemical is applied to the paper.
    - Pin punctures: Small pin punctures on selected letters are ordinarily not visible unless the paper is held infront of the light.
    - Type written correction ribbon: Used in between lines typed with a black ribbon, the results of the typing with the correction tape are visible only under a strong light.

Drawbacks of Steganography: Requires a lot of overhead to hide a relatively few bits of information. Once the sytem is discovered it becomes virtually worthless.

CONVENTIONAL ENCRYPTION

* Reffered to as Concetional/ Private-key/ Single-Key
* Sender and receipient share a common key
* All classical encryption algorithms are private-key was only the prior to invention of public key in 1970 plaint text(the original message).

Some basic terminologies used:

* Ciphertext: the coded message.
* Cipher: algorithm for transforming plaintext to cipher text.
* Key: info used in cipher known only to sender/receiver.
* Encipher: Converting plaintext to ciphertext
* Decipher: Converting ciphertext to plaintext
* Cryptography: Study of encryption principles/methods