**Ethical Hacking: Cryptography**

**1. Cryptography Basics**

**What does cryptography mean?**

Cryptography - conversion of data into a scrambled form; data is mathematically scrambled by sending it through an algorithm, which is guided by a key

Cryptography Uses - authentication, integrity, confidentiality, non-repudiation

Encryption - legible data -> cipher text

Decryption - cipher text -> legible data

**Different types of cryptography**

Symmetric Cryptography - uses the same key for encryption and decryption; secret/shared/private key cryptography; provides us confidentiality; there are no authentication, integrity, or non-repudiation

Asymmetric Cryptography - different keys are used to encrypt and decrypt; encryption uses public key; decryption uses private key; key pair - a pair of private and public keys; public keys are freely distributed (and with the private key, I can unlock all the encrypted message sent to me); provides confidentiality and authentication (since I have the key, I am in fact the recipient of the info)

Hashing - while symmetric and asymmetric algorithms go two ways, hashing goes one way; it takes data and scrambles it in a one way mathematical function into data that can never be decrypted

**2. Ciphers**

**Different types of ciphers**

Ciphers - algorithms used for encryptions and decryption

Plain text (original text); Algorithm (mathematical mutation that we perform on the plain text); Key (unique info that guides the mutation); Ciphertext (scrambled text)

Substitution Cipher - have the decoder ring & assign each letter to correspond to smth else

Transposition Cipher - transpose letters; keys are just numbers; you just shift the letters to the value of the key

XOR Cipher - uses lookup table to determine what the output is; using two sets of binary codes w a ^ in between, you can use the lookup table

Block Ciphers - encrypts finite block at once; must have all data prior to processing (that is, PDF or Word doc)

Stream - encrypts data continuously; works on data as it is received

**Symmetric encryption**

Symmetric Encryption Algorithm - computationally fast; referred to as "private key encryption"; scalability issues occur with large number of unique keys; max keys = N(N-1)/2

Symmetric Encryption Algorithm is not linear, meaning that the more people exist, the more out of control the number of keys get

Data Encryption Standard (DES) - symmetric; archetypal block cipher (works on finite size of data & size of input and output data is same); 64-bit chunks

Data Encryption Standard (DES) - some inherit weaknesses; not used for communication - it's commonly used to store things for a single user (computer); replaced by AES bc of the inherit weaknesses

Single DES -> Triple DES: using three keys to encrypt a file (when it's decrypting, uses the reverse key order of encryption)

Advanced Encryption Standard (AES) - symmetric; originally "Rijndael"; iterated block cipher (one operation repeated multiple times on same block of data); 128-bit blocks; key sizes: AES-128, AES-192, AES-256

Rivest Cipher (RC) - symmetric (RC itself is not a symmetric algorithm); general term for a family of ciphers designed by Ron Rivest (RC4, RC5, RC6)

RC4 - stream cipher (no need for finite data - used for ongoing communication); variable key size

RC5 - block cipher (need finite size of data to operate on); parameterized algorithm; variable block size; variable key size (0-2040 bits)

RC6 - built on top of RC5; additions: integer multiplication & 4x4 working registers

**Asymmetric encryption**

Asymmetric Encryption Algorithms - computationally slow; referred to as "public key encryption"; use large prime numbers in trapdoor functions (easy to do one way, but hard to do the other)

example: two prime numbers (2801 and 3347) -> 2801 \* 3347 = 9,374,947 -> it's easy to get the multiplication, but hard to find the two prime numbers that make up that number

Rivest-Shamir-Adleman (RSA) - asymmetric; most widely used authentication algorithm; use two very large prime numbers, up to 4096 bits, which can count as high as 1.04E1233; must determine the prime factors of product to crack

ElGamal - asymmetric; developed for digital signature usage; doesn't necessarily use prime numbers, but rather based on solving discrete logarithm problems

Elliptical Curve Cryptography (ECC) - asymmetric; performs discrete logarithm problems over points on an elliptic curve

Diffie-Hellman - asymmetric; used for key exchanges; used in protocols such as SSL and IPsec; drawback: susceptible to man-in-the-middle attacks

**Mixing asymmetric with symmetric**

Weakness in Symmetric - difficult to keep keys a secret; both parties have to have a hold of the keys without exposing it

Weakness is Asymmetric - no key exchange issue, but they are computationally intensive (infeasibly slow on large amounts of data)

Hybrid system (mixture of sym and asym) - recipient sends over public key, sender locks (encrypts) the symmetric key, the recipient unlocks the symmetric key (they are the only one with the private key to unlock it), now both the recipient and the sender has the symmetric key in a secure way