# CS 161 Final Cheat Sheet

## Kerchoff's Principle

You should not rely on the secrecy of the algorithm/protocol and or keysize, as wall as the possible plain text for security because eventually the adversary will figure them out.

## Mono-Alphabetic Ciphers: 1 to 1 mapping of characters to symbols

- Subsitution
  - Shift or Caesar's Cipher $E_k(m) \leftarrow m + k(\texttt{mod}\ N)$ $D_k(c) \leftarrow c - k(\texttt{mod}\ N)$
  - Affine Cipher: $E_k(m) \leftarrow k_{!}m + k_2(\texttt{mod}\ N)$ $D_k(c) \leftarrow k_{!}^{-1}(c - k(\texttt{mod}\ N)$
  - Substitution Ciphers have an extreme vulnerability to frequency attacks.

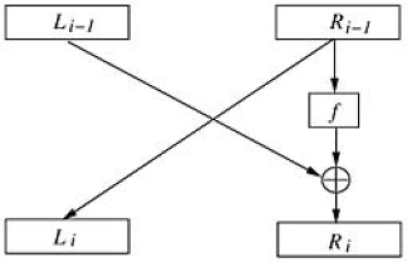
## Poly-Alphabetic Ciphers

- Vigenere Cipher: Shift by a repeated key
- Book Cipher (Beale Cipher) key is hidded in a passage of a set book.
- Vernam Cipher
  - Message is m bits and the key is n bits.
  - Bitwise xor the message and the key, if m is greater than n, then use the key multiple times.
- One-Time Pad
  - Same idea as the Vernam Cipher except we use a key that is the same length or greater than the length of the message, then discard it after each use.
- Transposition/Permutation Cipher
  - Break the message into n bit blocks, then on each block perfom the same permutation
  - Despite being polyalphabit, the cipher is still vulnerable to frequency attacks. Because the original patterns are still basically present. You can attack by checking anagrams.

## Data Encryption Standard (DES)

DES is a block cipher in which messages are divided into data blocks of a fixed length and each block is treated as one message either in M or in C. The DES encryping and decryption algorithms take as an input a 64-bit plaintext or ciphertext message and a 56-bit key, and output a 64-bit ciphertext or plaintext message. DES is done in 3 steps:

1. Apply a fixed "initial permutation" IP to the input block. $(L_0, R_0) \leftarrow IP(\texttt{Input Block})$ This step has no apparent cryptographic significance.
2. Iterate the following 16 rounds of operations (Feistel Cipher)



- the function is nonlinear and is considered a Substitution Cipher
- the move from $L_i \rightarrow R_{i-1}$ is a Transposition cipher
- Vernam cipher is used at the xor
- k is a 48 bit subsection of the 56 bit, "round key"

### Single DES

- vulnerable to brute force or exaustive key search attacks

### Triple DES

Triple DES uses an encryption-decryption-encryption scheme,
$c \leftarrow E_{k_1}(D_{k_2}(E_{k_1}(m)))$
$m \leftarrow D_{k_1}(E_{k_2}(D_{k_1}(m)))$
This scheme enlarges the keyspace while maintaining backward compatibility with single DES if $k_1 = k_2$

## Advanced Encryption Standard (AES)

AES is a block cipher with variable block size and variable keysize. (block size can be 128, 192, 256 bit)
AES has 4 states:

1. Sub Bytes State: nonlinear substitution on each byte
2. Shift Rows State: Transposition rearranges the order of elements in each row
3. Mix Columns State: Polynomial multiplication after converting column to polynomial.
4. Add Round Key State: adds elements of round key to the state, basically bitwise "OR"