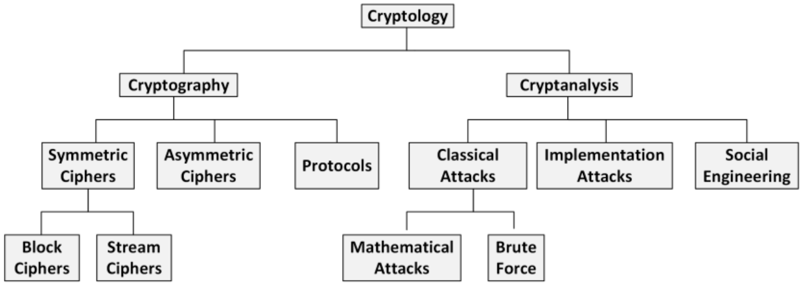
Lecture Notes on Nov/21

Cryptographic Algorithms

ECE217 Data Structure and Algorithms

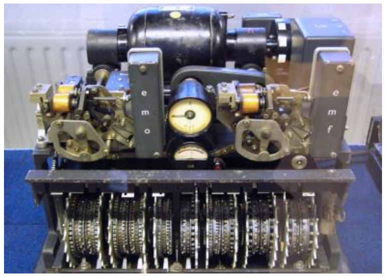
Instructor: Dr. Shayan (Sean) Taheri

Definitions and Goals


Cryptology
Cryptography
Cryptanalysis
Symmetric Ciphers
Asymmetric Ciphers
Protocols
Classical Attacks
Implementation Attacks
Social Engineering
Block Ciphers
Stream Ciphers
Mathematical Attacks
Brute Force

Definitions

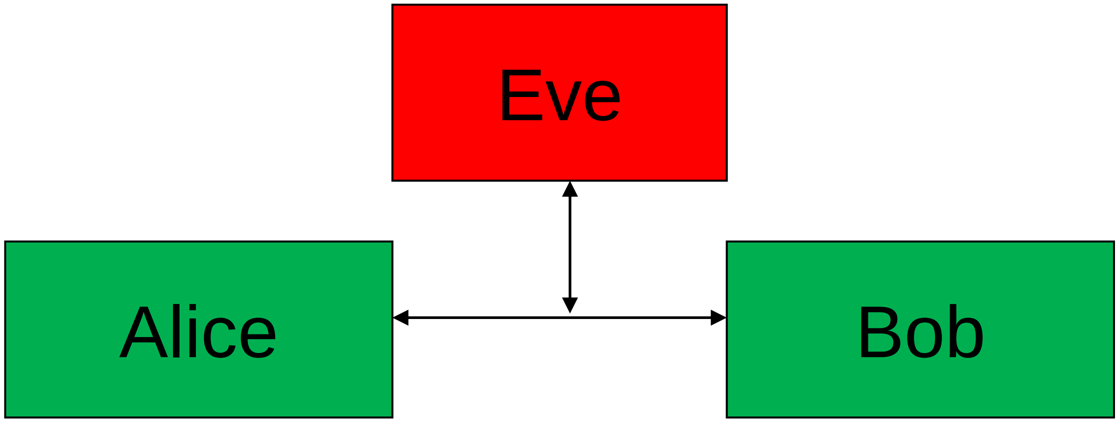
- Cryptography: The science (art) of encryption.
- Cryptanalysis: The science (art) of breaking encryption.
- Cryptology: Cryptography + Cryptanalysis.



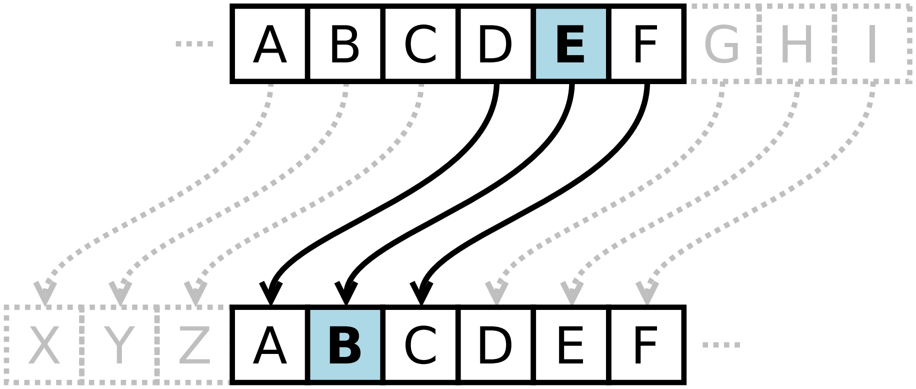
Lorenz cipher machine, used to encrypt communications.

Goals

- Encryption: To Prevent Intruder (e.g., Eve) from Intercepting Valid Message.
- Authentication: To Prevent Intruder from Impersonating Valid User (e.g., Alice or Bob).


Eve
Alice
Bob

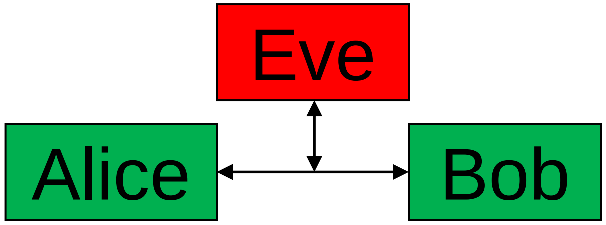
Insecure Channel



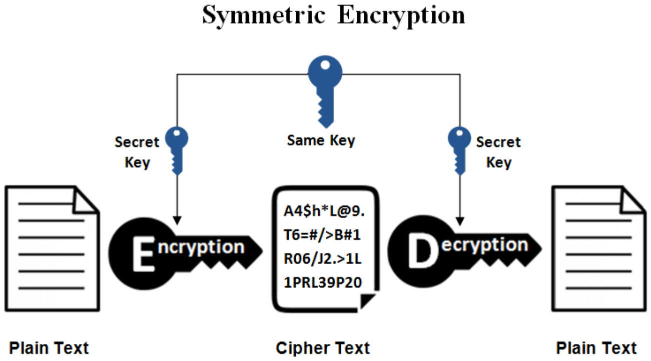
Alphabet shift ciphers are believed to have been used by Julius Caesar over 2,000 years ago. This is an example with k = 3. In other words, the letters in the alphabet are shifted three in one direction to encrypt and three in the other direction to decrypt.

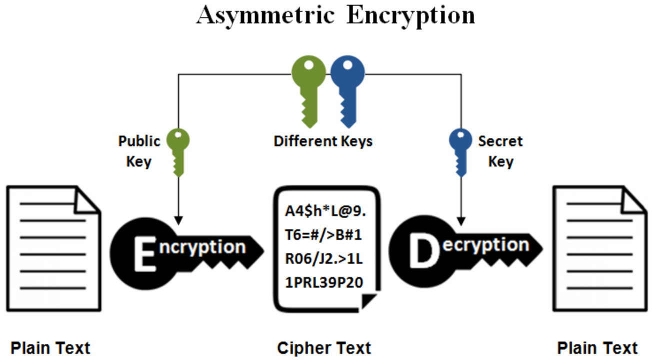
Symmetric/Secret/Private Key and Asymmetric/Public Key

- **Symmetric/Secret/Private Key for Encryption and Authentication**
  - Alice and Bob share a secret key, **Kab**.
  - **Encryption**: Plaintext message is encrypted and decrypted with **Kab**.
  - **Authentication**: Alice proves to Bob that she knows **Kab** (e.g., a password).
- **Public Key for Encryption**
  - Bob generates **2 keys**, **Keb** (**Public Key**) and **Kdb** (**Private Key**).
  - Bob publishes **Keb**.
  - Alice encrypts: **Ciphertext/C = Encryption/E (Keb, Plaintext/P)**.
  - Bob decrypts: **Plaintext/P = Decryption/D (Kdb, Ciphertext/C)**.
  - It must not be possible to compute **Kdb** (**Private Key**) from **Keb** (**Public Key**).



Insecure Channel


Symmetric Encryption

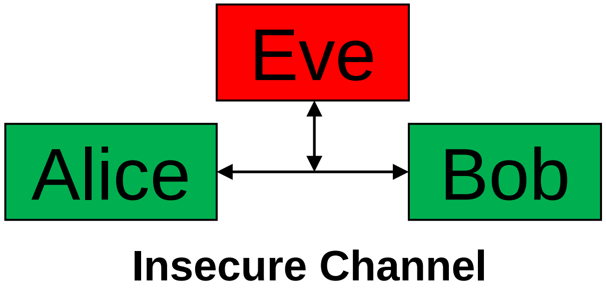

Asymmetric Encryption

Authentication by Digital Signature

- **Public Key for Authentication**
  - Alice generates **Kea** (**Public Key**) and **Kda** (**Private Key**).
  - Alice publishes **Kea** (**Public Key**).
  - Alice signs:

    (Plaintext/P, Signature/S) = DigitalSignature/DS (Kda, Plaintext/P).
  - Alice sends **(Plaintext/P, Signature/S)** to Bob.
  - Bob verifies:

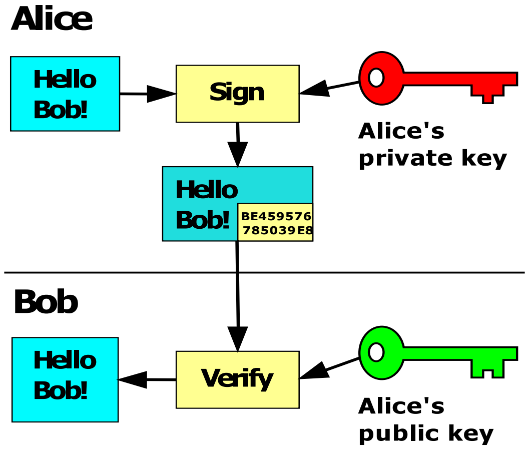
    Plaintext/P = DigitalVerification/DV (Kea, Signature/S) → Since only Alice knows **Kda** (**Private Key**).
- **Public Key for "<u>Encryption</u> + <u>Authentication</u>" Algorithm (Exercise).**


Eve

Alice

Bob

Insecure Channel


Alice

Hello Bob!

Sign

Alice's private key

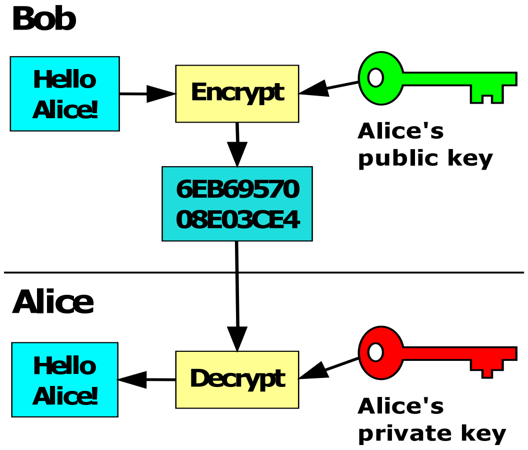
Hello Bob! BE459576 785039E8

Bob

Hello Bob!

Verify

Alice's public key


Bob

Hello Alice!

Encrypt

Alice's public key

6EB69570 08E03CE4

Alice

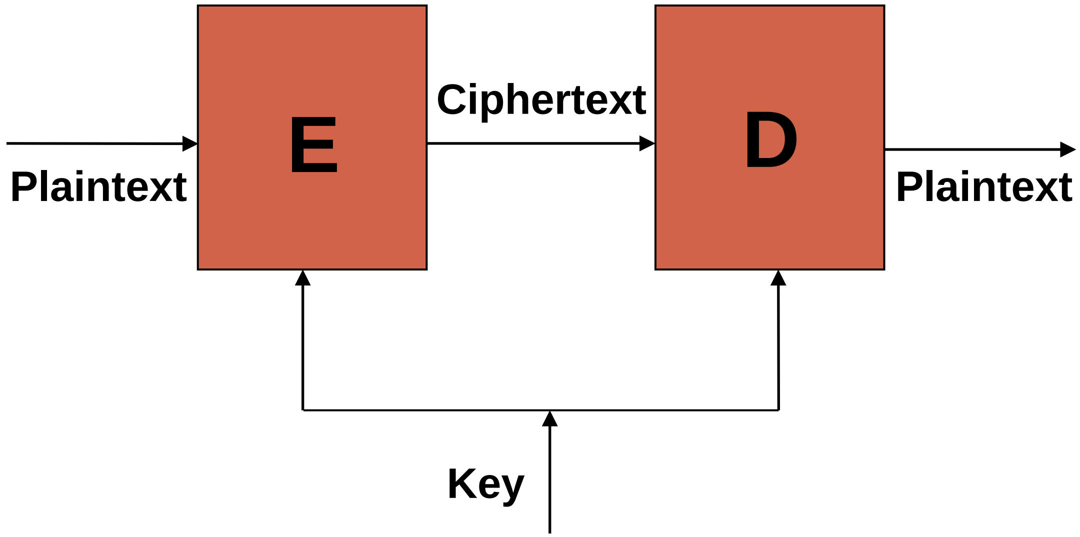
Hello Alice!

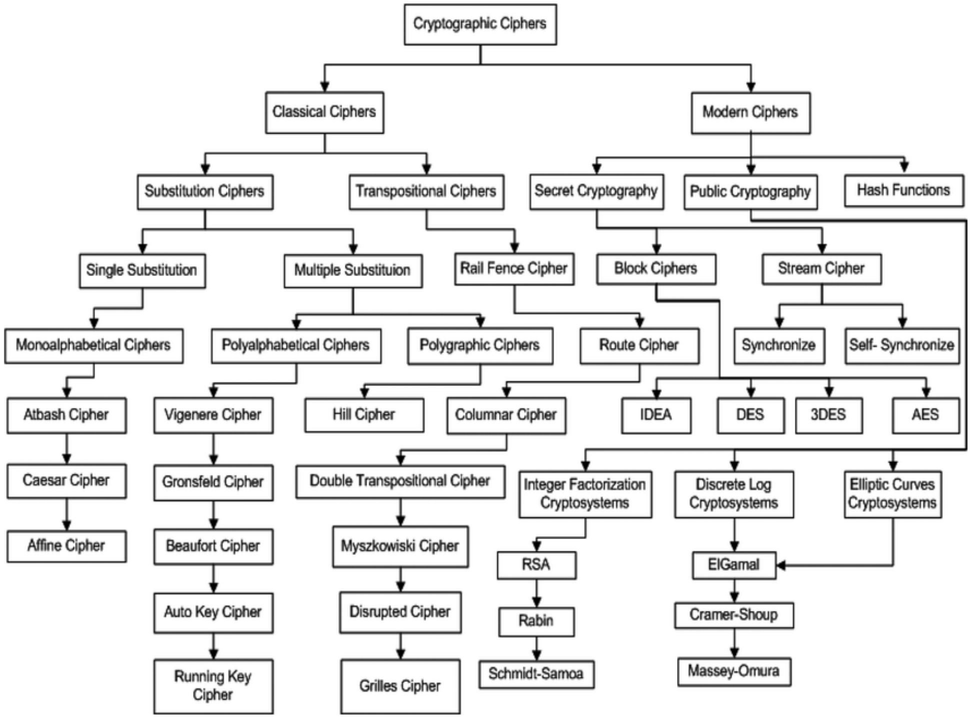
Decrypt

Alice's private key

Cryptographic Algorithms

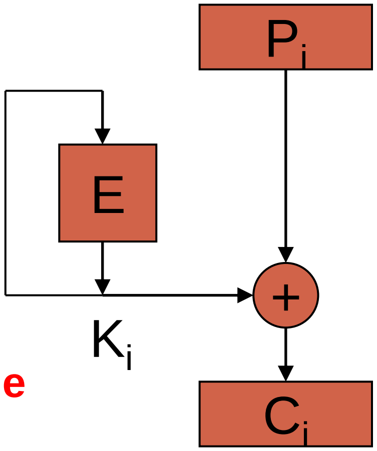
- **Types**
  - Symmetric/Private Key Encryption/Decryption (e.g., Block Ciphers).
  - Asymmetric/Public Key Encryption/Decryption.
  - Hash Function and Message Authentication Code.
  - Digital Signature.
- **Block Ciphers**
  - Example: AES, DES, 3DES, Two-fish, Blowfish, Serpent, RC4, IDEA.



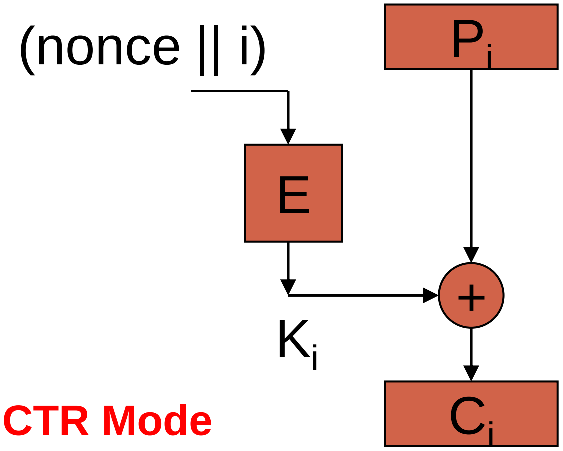


Block Ciphers – Modes

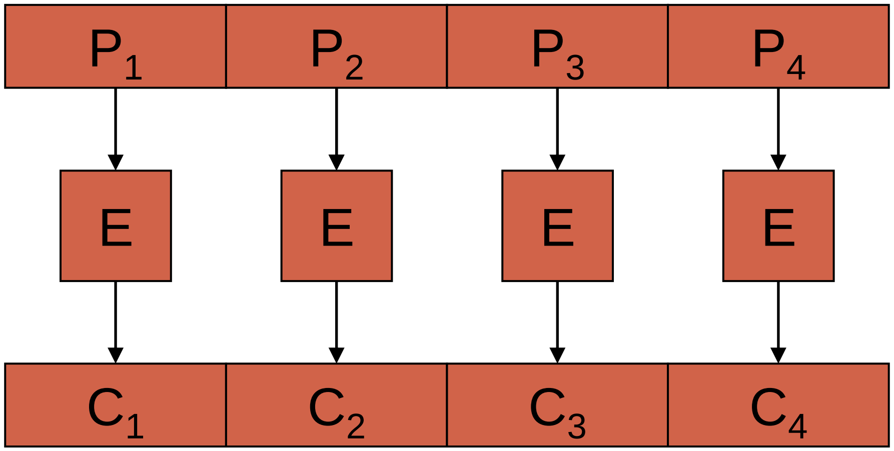
- **ECB - Electronic Code Book**: $C_i = E(K, P_i)$
- **CBC - Cipher Block Chaining:**
  - $C_i = E\ (K, P_i \text{ XOR } C_{i-1})$
  - $C_0 = IV$ (Initialization Vector: Fixed, random, counter, or nonce)
- **OFB - Output Feedback**
  - $K_0 = IV$ (nonce = Number used once)
  - $K_i = E\ (K, K_{i-1})$
  - $C_i = P_i \text{ XOR } K_i$
- **CTR – Counter**
  - $K_i = E\ (K, \text{nonce} \mid\mid i)$
  - $C_i = P_i \text{ XOR } K_i$



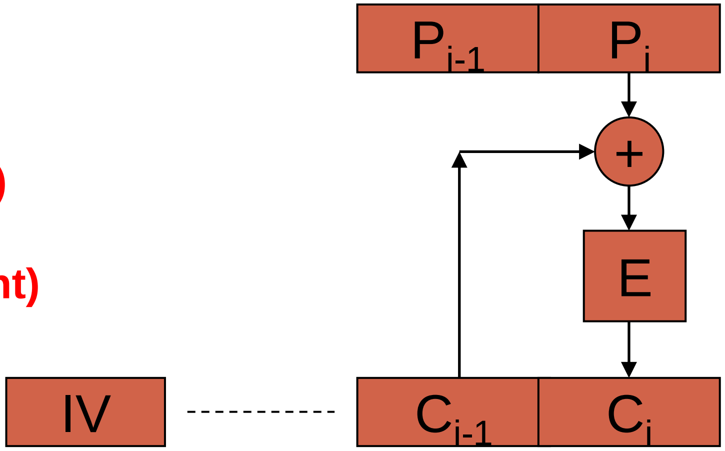
- OFB Mode



- CTR Mode



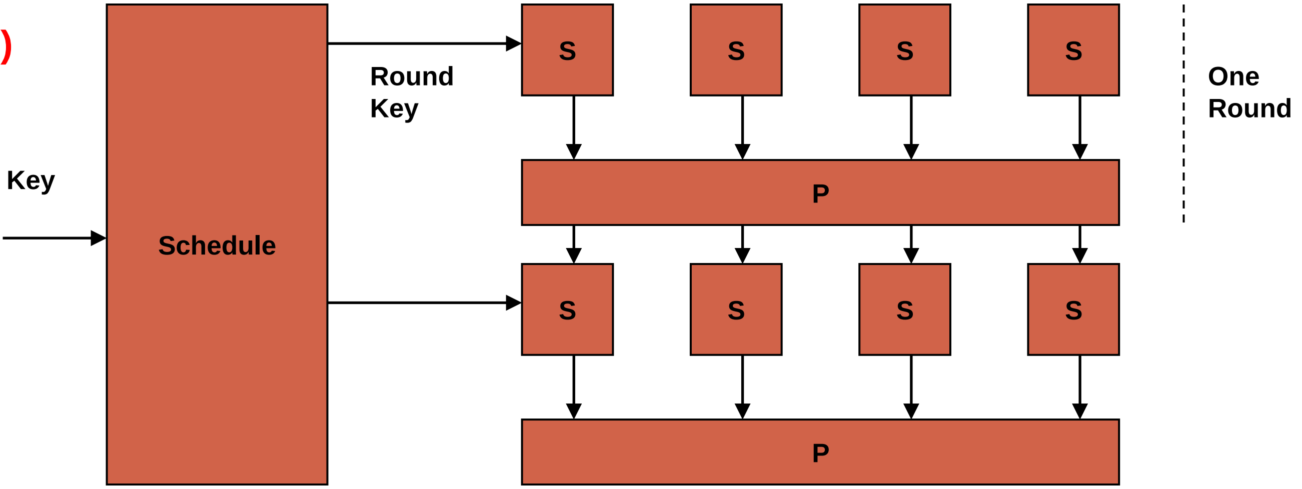
- ECB Mode (Left)
- CBC Mode (Right)

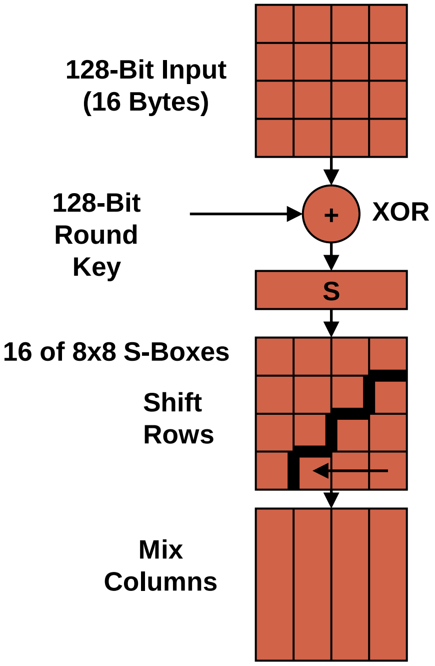


Block Ciphers – Architecture

- **Substitution/S Boxes**: Invertible lookup tables that they depend on key.
- **Permutation/P Boxes**: They reorder bits (may depend on key).
- **Key Schedule**: Function of key (e.g. bit selection or simple hash).

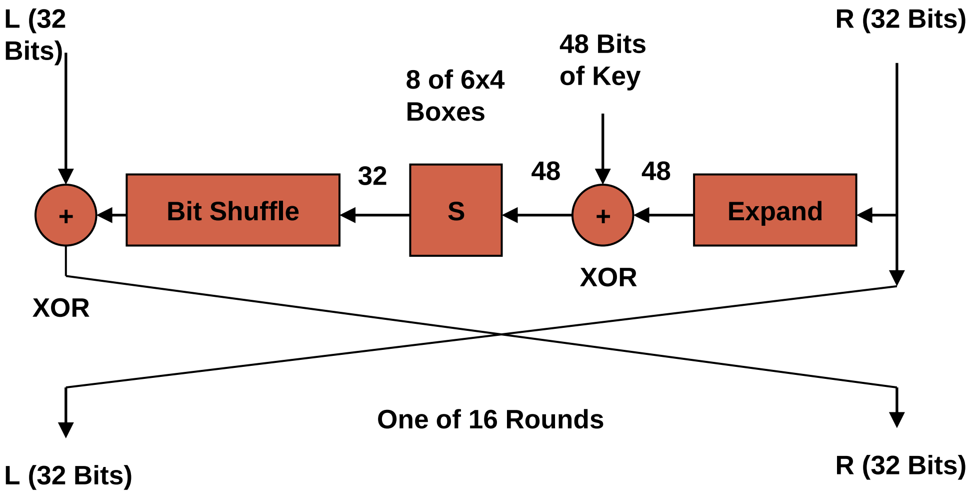
- Block Cipher Components (Top-Right)
- DES Round Network (Bottom-Right)
- AES Round Network (Bottom-Left)



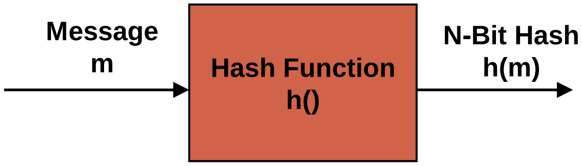


S(i) = k XOR rol(k,4) XOR rol(k,5) XOR rol(k,6) XOR rol(k,7) XOR 0x63, Where k = i^{-1} in GF(2^8),
rol = Rotate Byte Left

Multiply By M in GF(2^8) Over Polynomial $x^8+x^4+x^3+x+1$ Where M=
$$\begin{matrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{matrix}$$

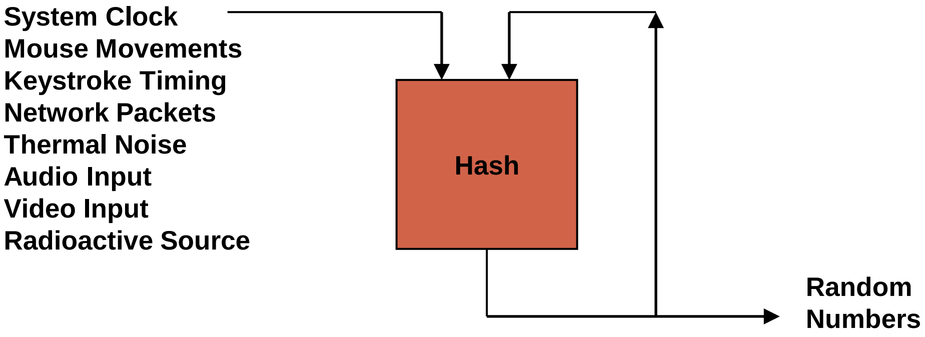


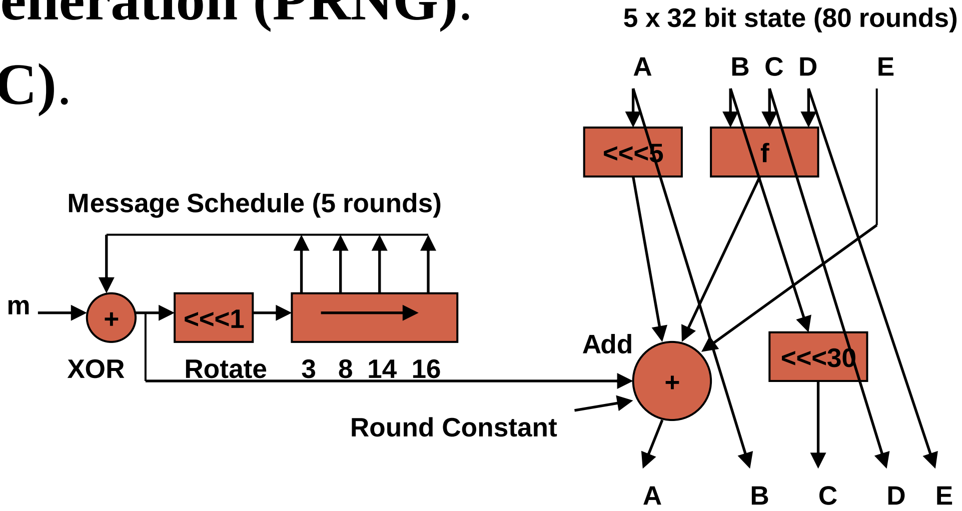
Secure Hash Function



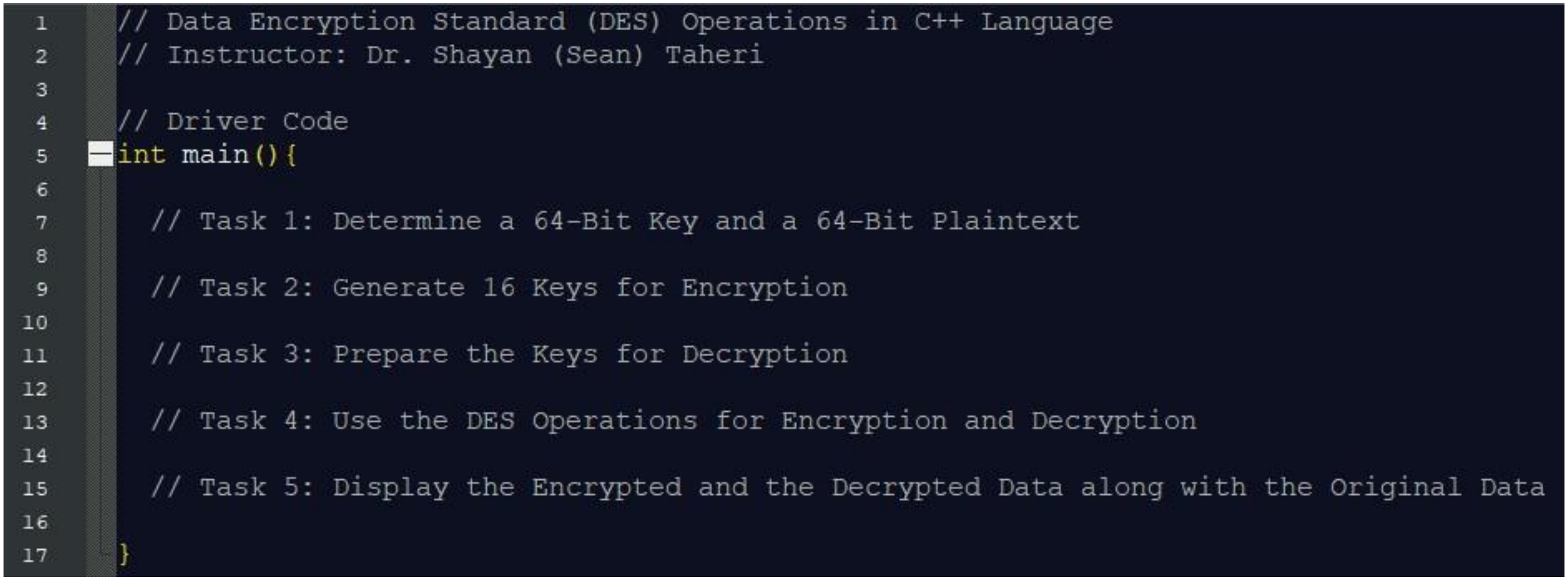
- **Goals**
  - **Collision Resistance**: It takes $2^{n/2}$ work to find any m_1, m_2 such that $h(m_1) = h(m_2)$.
  - **First Preimage Resistance**: Given h(m) it takes 2^n work to find m.
  - **Second Preimage Resistance**: Given m_1 it takes 2^n work to find m_2 such that $h(m_1) = h(m_2)$.
- **Applications**
  - **Faster Digital Signatures**: Alice signs h(P) instead of P.
  - **Password Verification** (e.g. UNIX) without Storing Passwords.
  - **Strong Pseudo-Random Number Generation (PRNG)**.
  - **Message Authentication Code (MAC)**.

- SHA-1 (Bottom-Right)
- PRNG (Bottom-Left)





DES Cryptographic Algorithm in C++ Language



```cpp
// Data Encryption Standard (DES) Operations in C++ Language
// Instructor: Dr. Shayan (Sean) Taheri

// Driver Code
int main(){

    // Task 1: Determine a 64-Bit Key and a 64-Bit Plaintext

    // Task 2: Generate 16 Keys for Encryption

    // Task 3: Prepare the Keys for Decryption

    // Task 4: Use the DES Operations for Encryption and Decryption

    // Task 5: Display the Encrypted and the Decrypted Data along with the Original Data

}
```

Assignment

- **Reading Assignment:**
  - Handbook of Applied Cryptography. First Edition. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone.
    - ✓ Chapter 1: Overview of Cryptography.
- **Assignment 3 Deadline**: **November/30/2022**.

Questions?