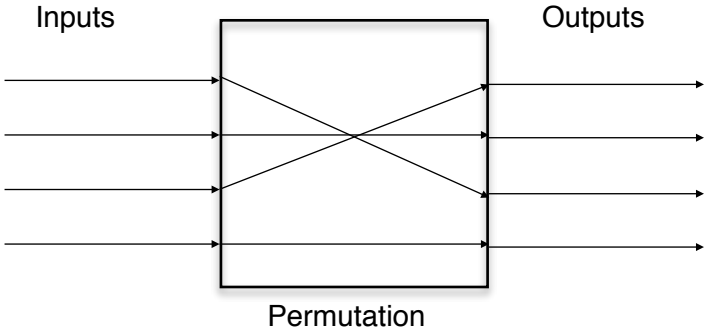
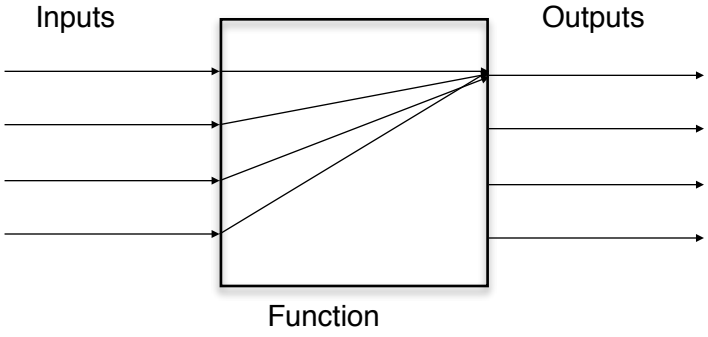
Lecture Scribe - Cyril Saade

Tuesday January 31st 2017

- **Correctness of encryption scheme:** $Dec_k(Enc_k(m)) = m$

$RandomPerm^{-1}(RandomPerm(m))$
^ decryption ^ encryption



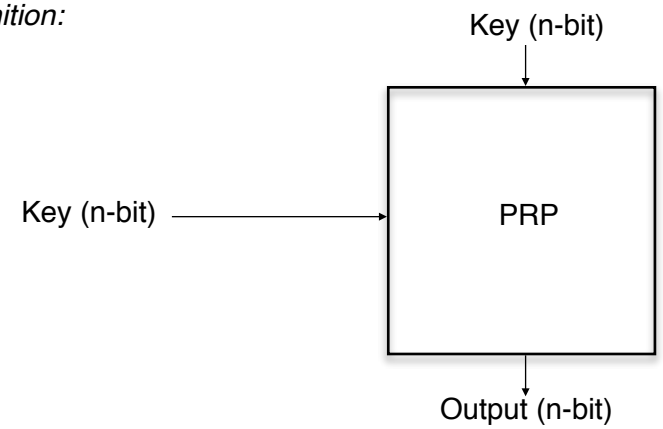


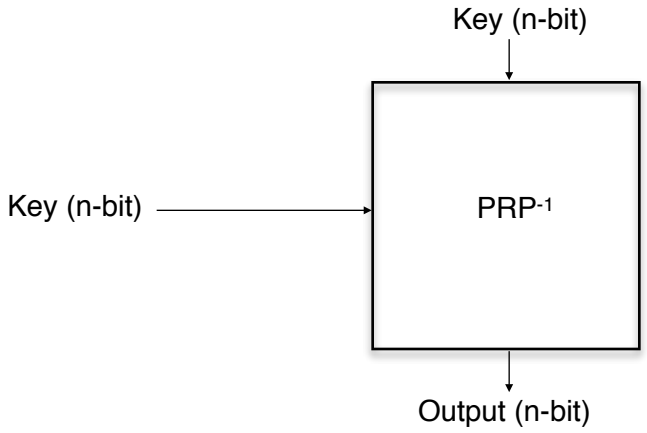
- Number of possibilities on n-bit input: $2^n!$
- Permutation is safer.

- **Pseudo-random permutation:**

Belief: AES is a Pseudo-random permutation (PRP) - 128-bit security level which is considered good.

Definition:





- **Encryption Scheme for n-bit messages:**

cipherText = PRP_k(plainText)
C = $Enc_k(m) = PRP_k(m)$

Example: Say key was 4-bits long - Can trivially break the encryption scheme
—> Attack: for all possible keys k (2^4=16 possibilities)
$PRP^{-1}{}_k(c)$ (stop when find a "valid looking" message)

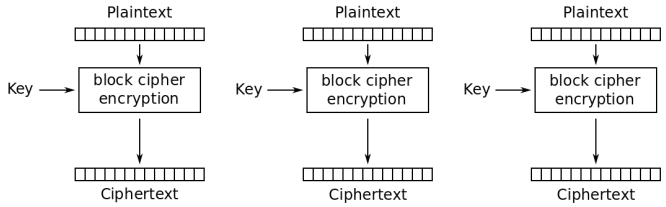
2^n! Possible permutations ~ $(2^n)^n$ representing my choice of random permutation
$\log_2(2^n)^n$ x $n2^n$. **Enough to stop brute force attacks.**

- **AES: Pseudo-random Permutation:**

Motivation: Attacker cannot distinguish between a world where we use AES, and another world where we use a Random Permutation. Explains the reason why AES is secure.

All of the techniques represent encryption schemes for an n-bit message. **What techniques do we use in order to encrypt multiple messages?**

- **Electronic Codebook:** break a message into n-blocks, and apply a block cipher with same key to every block.
    - Easily breakable: can apply frequency analysis. It is not secure enough

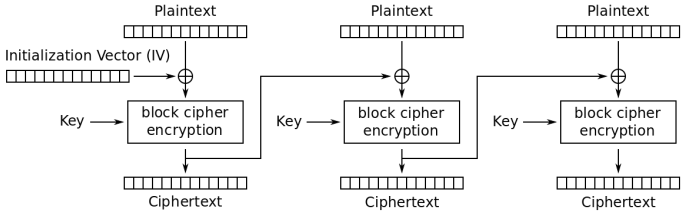


Electronic Codebook (ECB) mode encryption

Source: wikipedia

- **Cipher Block Chaining (CBC):**

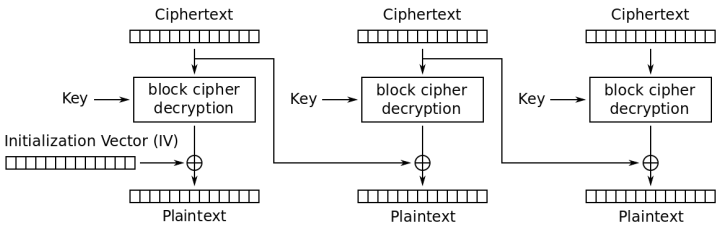
1. Encryption



Cipher Block Chaining (CBC) mode encryption

Source: wikipedia

2. Decryption



Cipher Block Chaining (CBC) mode decryption

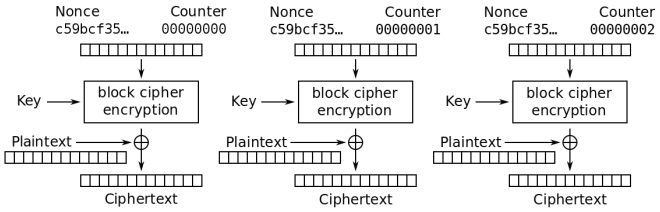
Source: wikipedia

Note: the initialization vector is exchanged as part of the ciphertext.

- **Counter CTR:**

Nonce: fresh random number (should be unique -> very low probability of collision)

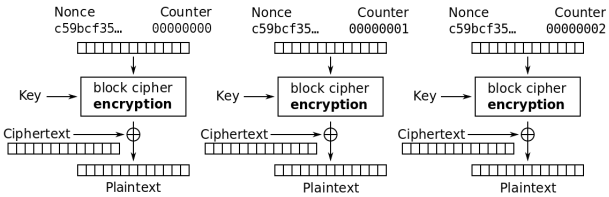
1. *Encryption*



Counter (CTR) mode encryption

Source: wikipedia

2. *Decryption*



Counter (CTR) mode decryption

Source: wikipedia