

## Review:

- Converting PRG => Stream Cipher does not work
- PRF with PRG => Stream Cipher works and is good
- CTR with PRF => RoR Secure Encryption
  - In CTR with PRF scheme, both encryption and decryption are done in the forward direction, which implies that the key generation scheme need not be invertible, it just needs to be deterministic so that the receiver can generate the same key-stream from the IV as the sender did.

## Today:

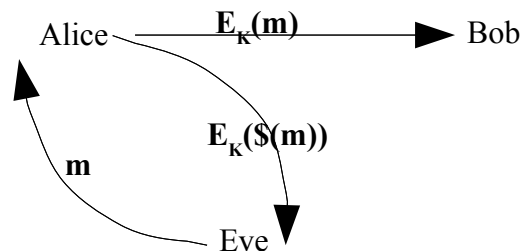
- CBC with PRP => RoR Secure
- The following terms all represent same security property
  - Semantically Secure  $\Leftrightarrow$  RoR Secure
  - $\Leftrightarrow$  Left or Right Secure
  - $\Leftrightarrow$  IND-CPA

In all these definitions, the adversary is given access to the encryption oracle but not to the decryption oracle. e. g. for RoR Security we require that  $E_K \sim E_K \circ \$$

## Notation: $\$(x)$

Random, non-deterministic string of the length of string  $x$ .

## Argument for desirability of non-determinism for $\$$ :



1. If  $\$$  is randomized then deterministic encryption is not secure because Alice, by sending the same message multiple times and looking at the returned ciphertext, can know which world she is in.
2. If  $\$$  is deterministic then for a deterministic encryption, Eve may or may not know which world she is in.

Because for our model, we want deterministic encryption to be insecure, we take  $\$$  to be non-deterministic(randomized).

**Remark:** We extensively talk about deciphering the world in order to prove our encryption scheme secure because any successful attack will decipher the world the system is in and by contra-positive, if we cannot decipher the worlds, there cannot be any successful attack on the system.

## CBC with PRP:

### Def: PRP

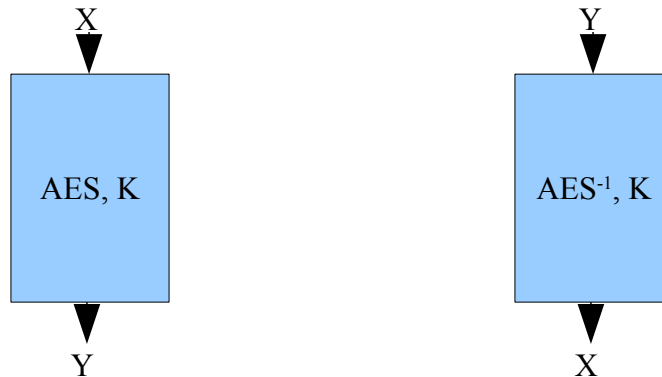
A function  $F: \text{keys} \times X \rightarrow X$  is a  $(t, q, \epsilon)$  PRP if for all adversaries running in time  $\leq t$  and making at most  $q$  oracle queries,

$$|\Pr [A^{FK} = 1 \mid k \leftarrow \text{keys}] - \Pr [A^P = 1 \mid P \leftarrow \text{Perms}(X)]| \leq \epsilon$$

In comparison to a PRF, a PRP never has a collision and hence is invertible. Another difference is that a PRP has the same set as its domain and co-domain, while PRF has different sets. In essence, PRP takes a string from a set as input and outputs another string from the same set deterministically and uniquely. The inverse function just takes the output string and gives the input string back.

### Examples:

1. AES:  $\{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$
2. DES:  $\{0,1\}^{56} \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$
3. RC5
4. Twofish



### Cipher Block Chaining (CBC) Mode:

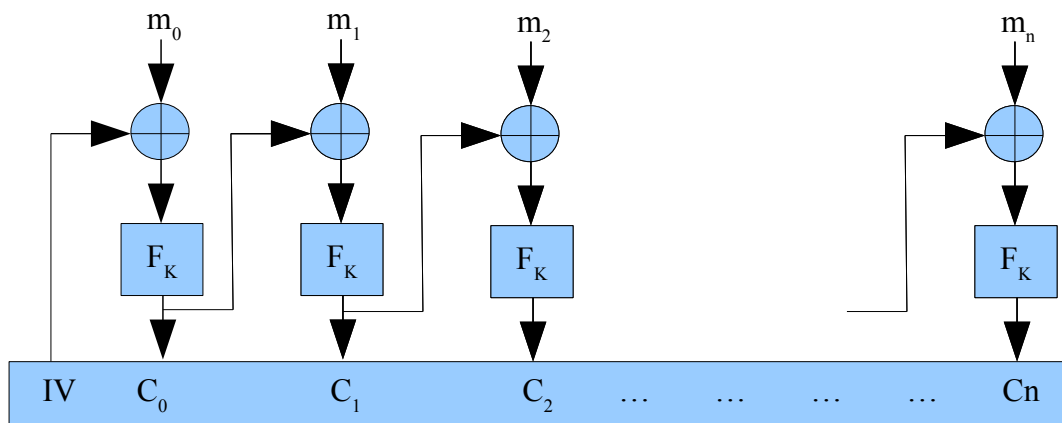
Due to the invertibility property, a PRP can be used for encryption in the CBC mode. The idea behind CBC mode is to divide a long message into blocks of the size of input of the PRP and chain these blocks together such that for each block of the message, the input to the PRP is the XOR of the ciphertext of the last block and the plaintext of current block. This way we achieve a non-deterministic encryption scheme. For the first block the XOR of an IV and the plaintext of the first block is used as the input. For decryption, the decryption algorithm is run on the ciphertext and the output of the decryption algorithm XORed with the ciphertext of the previous block.

In this scheme it is required to send the IV securely because an attacker can change arbitrary bits in the first block of the message by changing corresponding bits in the IV.

In CBC mode, the decryption can be parallelized because all the ciphertext blocks are available at the start but encryption cannot be parallelized. This behavior is different from the CTR mode where both encryption and decryption could be fully parallelized.

The same two strategies for picking the next IV can be followed:

- **CBC<sup>F</sup>**: IV is set to the current counter value and increased for each message.
- **CBC<sup>S</sup>**: IV is chosen randomly for each message.



**Encryption using a PRP( $F_K$ ) in CBC mode**

**Theorem:**

CBC $^F$  is  $(t - O(q), q, \epsilon + (q^2 / 2^{n+1}))$  RoR Secure if  $F$  is a  $(t, q, \epsilon)$  PRP, where  $n$  is the length of the IV.