MAD 4471: Cryptography and Coding Theory **Fall 2020**

Lecture 3: Block Ciphers

Lecturer: Jean-François Biasse *TA: William Youmans*

3.1 Pseudo - Random Functions (PRF)

A PRF is simply $S : \mathcal{X} \times \mathcal{K} \mapsto \mathcal{Y}$ efficiently evaluable.

Definition 3.1 (Informal) *A secure PRF is a PRF that "looks random".*

To formalize the fact that a PRF F "looks random", we put the adversary in front of a black box that evaluates F (Experience 0) and in front of a black box that evaluates a random function (Experience 1). The advantage of an adversary is its difference in terms of behavior (but not the answer itself).

Figure 3.1: Experiment 0

CHALLENGER		ADVERSARY
$k \xleftarrow{\mathcal{R}} \mathcal{K}$.	$\xleftarrow{x_1,\dots,x_g}$	Choose $x_1, \dots, x_g \in \mathcal{X}$
Computes $y_1, \dots, y_g$ with $y_i := F(x_i, k)$.	$\xrightarrow{y_1,\dots,y_g}$	Returns 0 for "random" and 1 otherwise

Figure 3.2: Experiment 1

CHALLENGER		ADVERSARY
$f \xleftarrow{\mathcal{R}} \text{Func}(\mathcal{X}, \mathcal{Y})$.	$\xleftarrow{x_1,\dots,x_g}$	Choose $x_1, \dots, x_g \in \mathcal{X}$
Computes $y_1, \dots, y_g$ with $y_i := f(x_i)$.	$\xrightarrow{y_1,\dots,y_g}$	Returns 0 for "random" and 1 otherwise

Definition 3.2 (Advantage against a PRF) *Let W_0 be the event "A returns 0 in Exp 0" and W_1 be the event "A returns 0 in Exp 1". The advantage of an efficient algorithm $\mathcal{A}$ against $\mathcal{F}$ is defined by*

$$Adv_{PRF}[\mathcal{A}, \mathcal{F}] := |Pr_{k \leftarrow \mathcal{K}}(W_0) - Pr_{f \leftarrow \text{Func}(X,Y)}(W_1)|.$$

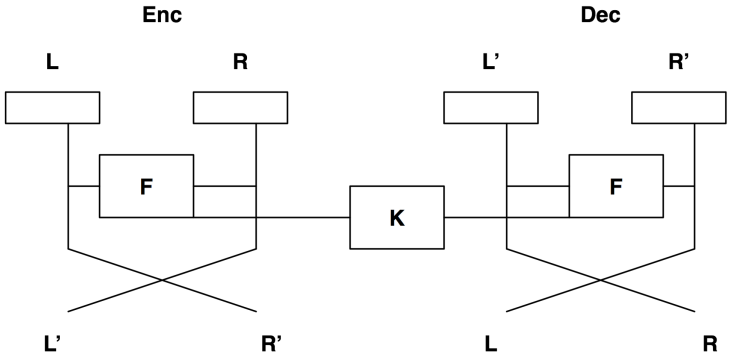
As usual, the PRF F is secure if $Adv_{PRF}(\mathcal{A}, \mathcal{F})$ is negligible for all efficient adversaries.

3.2 Block ciphers

A typical example of a PRF is a block cipher. By definition, it is a function $Enc : X \times \mathcal{K} \mapsto X$ that has a decryption function $Dec : X \times \mathcal{K} \mapsto X$ satisfying $Dec(Enc(x, k), k) = x$. It is secure if it "looks random".

Example 1 *A typical example of a block cipher is the DES (Data Encryption Standard). It is made of successive rounds of the block cipher in Figure 3.2. The blocks $S_1, S_2, \cdots, S_8$ are non linear (S-boxes) to prevent the whole function from being linear.*

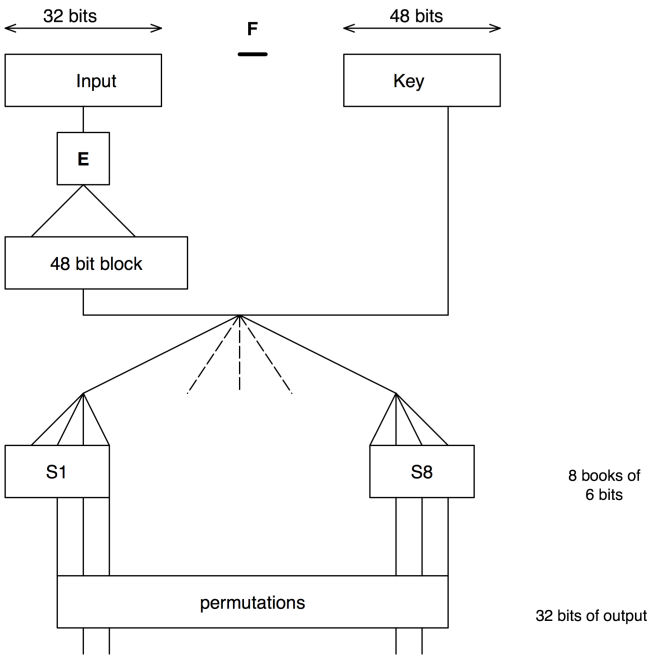
Figure 3.3: One round of the DES



The current standard of block ciphers is the Advanced Encryption Standard (AES). AES is the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. It encrypts blocks of 128 bits with keys of length 128, 192 and 256 bits. The previous standard was the Data Encryption Standard (DES) that has been now phased out.

A block cipher is a pseudo random permutation. Indeed, since we require the existence of a decryption function, the encryption function must be a permutation. However, we want it to be secure as a pseudo random function. This is not completely straightforward as permutations have a distinctive characteristic: if $x_1 \neq x_2 \neq \cdots, \neq x_q$, then $f(x_1, k) \neq f(x_2, k) \neq, \cdots, f(x_q, k)$. The adversary can request evaluations at all $x_i \in \mathcal{X}$ and check if they are all different. If it is the case, the adversary returns '0'. The proportion of permutations among all functions $\mathcal{X} \to \mathcal{X}$ is small as $|\mathcal{X}|$ grows, making the advantage of the adversary better. Fortunately, this test requires a lot of effort to the edversary as $|\mathcal{X}|$ grows to infinity. An efficient adversary cannot request more than a reasonable number q of evaluations. If $|\mathcal{X}| = 2^{80}$ (for example), then $q \ll |\mathcal{X}|$ (as we assume that an efficient adversary would only handle 2^{30} operations). To formalize this, we can introduce the notion of secure Pseudo Random Permutation (PRP). A PRP $f : \mathcal{X} \times \mathcal{K} \to \mathcal{X}$ said to be secure if there is no efficient adversary against f in the modified PRF security game where in Experiment 1 the challenger draws a random function among the permutations of $\mathcal{X}$ (in which case being a permutation does not identify f. As $|\mathcal{X}|$ grows, the two notions of security get more and more similar, as formalized by the PRF switching lemma.

Figure 3.4: The Feistel function F occurring in the DES



Lemma 3.3 (PRF switching lemma) *Let $f : \mathcal{X} \times \mathcal{K} \to \mathcal{X}$ be a pseudo random permutation. Then for any q-query adversary $\mathcal{A}$,*

$$|\mathrm{Adv}_{\mathrm{PRF}}(\mathcal{A}, f) - \mathrm{Adv}_{\mathrm{PRP}}(\mathcal{A}, f)| < \frac{q^2}{2|\mathcal{X}|}.$$

3.3 Modes of operation

Block ciphers are designed to encrypt only small blocks of message. For example the DES encrypts blocks of 64 bits while its successor the AES (Advanced Encryption Standard) encrypts blocks of 128 bits. We want to be able to use block ciphers for messages of arbitrary length. To do this, we need to use of the of various *modes of operations* that are available. The most obvious way of encrypting a long message using a block cipher is to use the Electronic Codebook mode (ECB). The message is broken into blocks that are encrypted independantly.

This construction is simple, and its evaluation can be trivially parallelized, but it is unfortunately not semantically secure. Indeed, an adversary for the Chosen Plaintext Attack security game can choose m_0 of the form $m_0 = m||m$ (the concatenation of two identical blocks) and m_1 of the form $m_1 = m||m'$ for $m \neq m'$ (the concatenation of two different blocks). Then when the adversary receives an encryption c, they know how to determine if $c = Enc(m_0, k)$ of $c = Enc(m', k)$. If $c = c_0||c_0$ (concatenation of two identical blocks), then c has to be the encryption of m_0. Otherwise, it is the encryption of m_1. Encryptions of pictures with many pixels of the same color are a perfect illustration of this semantic insecurity.

Figure 3.5: Electronic Codebook mode (ECB)

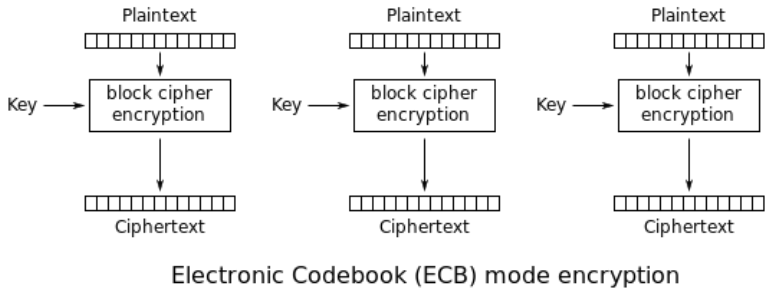
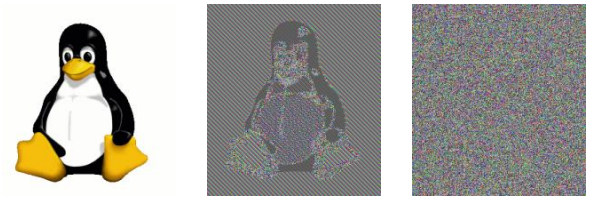


Figure 3.6: Encryption with the ECB mode (middle) compared with a secure mode (right)

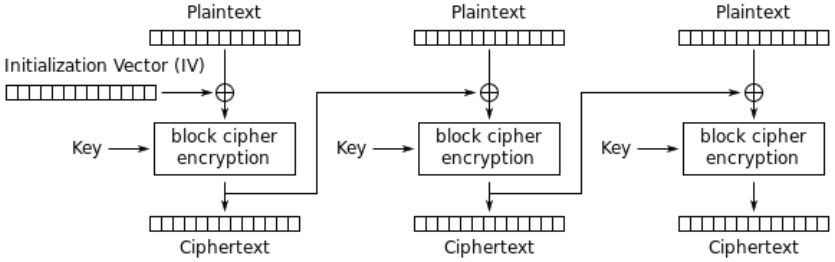


The Cipher Block Chaining mode (CBC) uses the encryption of the previous block to encrypt the next one. It is semantically secure if the corresponding block cipher is secure.

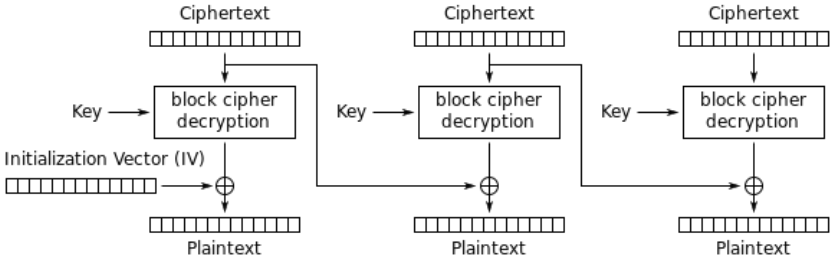
The counter mode (CTR) is interesting in the sense that it provides a way to turn a block cipher into a stream cipher. To do this, we simply encrypt $1, 2, \cdots, k$ to produce the keystream, which we then XOR to the message.

Remark 1 *In the CBC mode, there is an IV (initial value), and in the CTR mode, each block is encrypted using a nounce value. These values have the same puropose: providing semantic security in the context of many-times key (which we have not discussed here). To have semantic security in a context where the same key is used multiple times, we must ensure that two consecutive encryptions of the same message m give two different ciphertexts. This is ensured by choosing random IV (or nounce) for every new encryption. If we do not do that, then an adversary who plays the CPA security game multiple times with the same key can choose the same message m and win the game as all the encryptions of m are the same.*

Figure 3.7: Cipher Block Chaining mode (CBC)

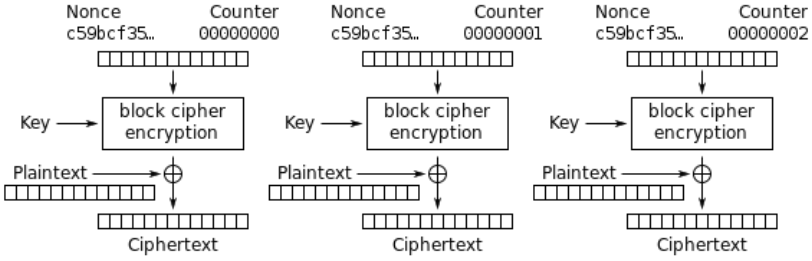


Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Figure 3.8: Counter mode (CTR)



Counter (CTR) mode encryption