COMP 8920: Cryptography Winter 2025

Lecture 8 — Jan 30, 2025

Prof. Curtis Bright *Scribe: Aidan Bennett*

1 Overview

In the last lecture we introduced block ciphers, and the DES cryptosystem.

In this lecture we continue our discussion of the DES cryptosystem, and the cryptosystem that eventually replaced it; AES.

2 DES (continued)

DES has 16 rounds, uses a block length of 64 bits, and a key length of 56 bits. A permutation is applied to the state before and after the cipher, however, this does not affect the cryptanalysis. Each k^i (ith round key) is a permutation of 48 bits, taken from the key k. The function $f : \mathbb{Z}_2^{32} \times \mathbb{Z}_2^{48} \to \mathbb{Z}_2^{32}$ takes as input the right half of the current state, and the round key. $f(A, J)$ is evaluated as follows:

1. An fixed expansion function $E : \mathbb{Z}_2^{32} \to \mathbb{Z}_2^{48}$ is applied to A. This is simply a permutation of the 32 bits, with 16 of the bits appearing twice.
2. $E(A) \oplus J$ is computed, and the result is written as the concatenation of 6-bit strings B_i; $B = B_1B_2B_3B_4B_5B_6B_7B_8$ (48 bits total).
3. Eight s-boxes are applied, where $s_i : \mathbb{Z}_2^6 \to \mathbb{Z}_2^4$ maps the 6 bits from B_i to 4 bits, denoted C_i. We write the result as $C = C_1C_2C_3C_4C_5C_6C_7C_8$ (32 bits total).
4. The permutation P is then applied to C, and the resulting $P(C)$ is the output of the function ($P(C) = f(A, J)$).

This can be visually seen in the diagram in Figure 1.

When first proposed, DES was criticized for consisting of mostly linear operations. The only nonlinear operations are the s-boxes. This was seen as an issue as linear functions are easily invertible. Further, a keyspace of size 2^{56} is not safe from brute force search.
To demonstrate this point, a $250K machine was built in 1998 that was capable of searching 88 billion keys per second. It was able to break DES via a known plaintext attack in 56 hours. Again in 1999, a distributed effort among 100,000 PCs was able to break DES in as little as 22 hours.

3 Advanced Encryption Standard (AES)

As a result of these insecurities, DES was replaced by the Advanced Encryption Standard (AES) in 2001. AES uses a block length of 128 bits, and a key length of either 128, 192, or 256 bits, with

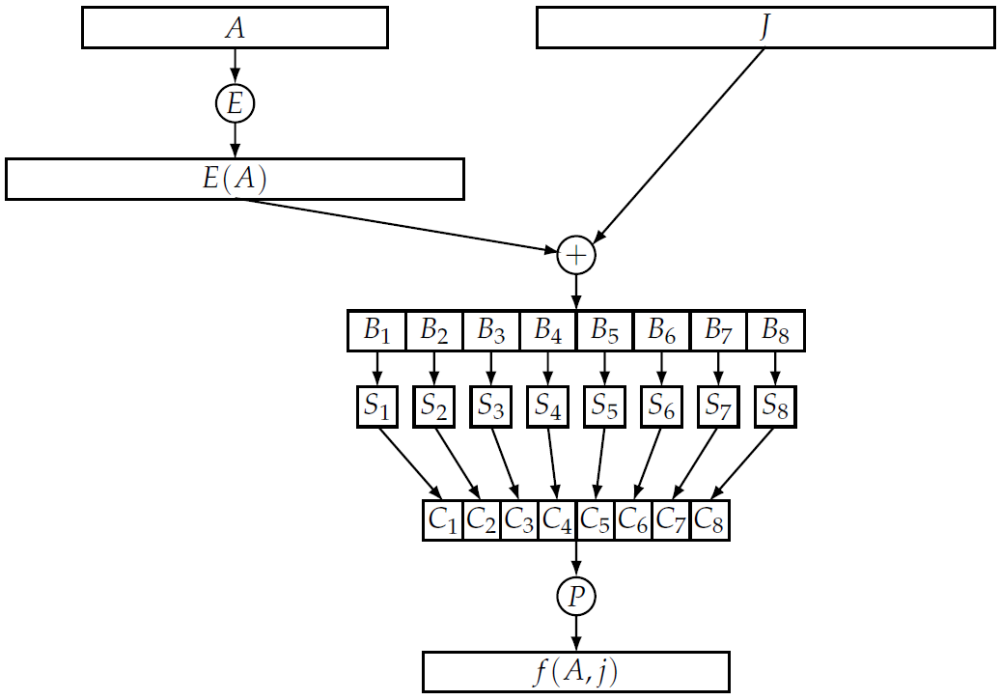

Figure 1: DES f function, from *Cryptography, Theory and Practice*, 4th edition, by Douglas R. Stinson and Maura B. Paterson

10, 12, or 14 rounds, respectively. The steps of AES are as follows:

1. Given plaintext x, initialize **state** to x, and XOR it with the round key.
2. For each round:
   (a) Perform substitution on **state**
   (b) Perform the linear operation "mixcolumns" on **state**
   (c) XOR state with round key
3. Define the ciphertext y to be the current **state**.

The **state** is represented by a 4×4 matrix of bytes. The initial **state** given plaintext $x_0, \ldots, x_{15}$ would be

$$\begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix}$$

The s-boxes apply to each byte of the state independently. In contrast to DES, s-boxes of AES can be defined algebraically from a finite field. Byte $a_7 a_6 \ldots a_0$ is transformed into the element $\sum_{i=0}^{7} a_i x^i$ in the field $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/\langle x^8 + x^4 + x^3 + x + 1 \rangle$, and all operations are done in the field to define the s-box output.

The permutations of **state** shift the rows cyclically to the left, i.e.:

$$\begin{bmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \end{bmatrix} \longrightarrow \begin{bmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_5 & s_9 & s_{13} & s_1 \\ s_{10} & s_{14} & s_2 & s_6 \\ s_{15} & s_3 & s_7 & s_{11} \end{bmatrix}$$

The "Mixcolumns" operation is carried out on each column independently, where each column is replaced by a new column obtained by multiplying the original column by particular matrix of elements in $\mathbb{F}_{2^8}$. The round keys are given by expanding the 128-bit key into 44 4-byte words $w[0], \ldots, w[43]$, where the round key k^i is given by $w[4i], \ldots, w[4i+3]$. These are computed via cyclic shifts of the word bytes as well as s-boxes. The decryption of AES simply applies all the same steps in reverse.

3.1 Modes of Operation

There are several standard ways of using a block cipher like DES/AES.

- **Electronic Codebook (ECB):** Given a sequence $x_1, \ldots$, each x_i is encrypted with the same key k to generate $y_1, \ldots$. The main drawback of the ECB mode is that identical plaintext blocks encrypt to identical ciphertexts.
- **Cipher block chaining (CBC):** Each ciphertext block y_i is XORed with the following plaintext block x_{i+1} before encryption with the key. An initialization vector (IV), is typically chosen randomly, and is sent in the plaintext and forms the base case y_0. y_i is computed via $y_i = e_k(y_{i-1} \oplus x_i)$.
  As a result, *any* change in x_i will change y_k, for all $k \geq i$. So a MAC (message authentication code) can be applied to any set of plaintexts, stating the source of the message. This ensures message integrity.
- **Output feedback (OFB):** A keystream $z_1, \ldots$ is generated via $z_i = e_k(z_{i-1})$, where $z_0 = \text{IV}$, the initialization vector. The plaintext is then encrypted via $y_i = x_i \oplus z_i$. Similar to a steam cipher.
- **Cipher feedback (CFB):** Also like a stream cipher, but asynchronous (z_i's depend on x_i's). Start with $y_0 = \text{IV}$ and produce the keystream z_i via $z_i = e_k(y_{i-1})$, and $y_i = x_i \oplus z_i$.
- **Counter (CTR):** Also behaves like a stream cipher, but the keystream is constructed from encrypting a sequence of counters using the key k. We choose counter **ctr** and a bitstring of length m (the block length). Then, a sequence of counters $T_i = \mathbf{ctr} + i - 1 \mod 2^m$. Encryption is done via $y_i = x_i \oplus e_k(T_i)$, like in OFB. An advantage of CTR mode is that the keystream can be computed in parallel, as computing $e_k(T_i)$ does not require knowledge of $e_k(T_{i-1})$.