EE 720: An Introduction to Number Theory and Cryptography (Spring 2020)

Lecture 8 — February 6, 2020

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Prove the CPA-security of the encryption scheme presented in the last lecture.
- Define pseudorandom permutations
- Describe the construction of DES

2 CPA-Secure Encryption from Pseudorandom Functions

- Let F be a length-preserving pseudorandom function. Define a private-key encryption scheme for messages of length n as follows:
  - `Gen`: On input 1^n, choose k uniformly from $\{0,1\}^n$.
  - `Enc`: Given $k \in \{0,1\}^n$ and message $m \in \{0,1\}^n$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext
  $$c := \langle r, F_k(r) \oplus m \rangle.$$
  - `Dec`: Given $k \in \{0,1\}^n$ and ciphertext $c = \langle r, s \rangle$, output the plaintext message
  $$m := F_k(r) \oplus s.$$

Theorem (Thereom 3.31 of KL)**.** *If F is a pseudorandom function, then the above construction is a CPA-secure private-key encryption scheme for messages of length n.*

Proof. Done in class. □

3 Pseudorandom Permutations

- In practice, constructions of pseudorandom permutations are used instead of pseudorandom functions.
- Let $\texttt{Perm}_n$ be the set of all permutations (bijections) on $\{0,1\}^n$. An $f \in \texttt{Perm}_n$ can be seen as a lookup table where any two distinct rows must be different.
- $|\texttt{Perm}_n| = (2^n)!$
- A function $F : \{0,1\}^{l_{key}(n)} \times \{0,1\}^{l_{in}(n)} \to \{0,1\}^{l_{in}(n)}$ is called a *keyed permutation* if for all $k \in \{0,1\}^{l_{key}}(n)$, F_k is a permutation.

- $l_{in}(n)$ is called the *block length* of F.
- F is *length-preserving* if $l_{key}(n) = l_{in}(n) = n$.
- F is said to be *efficient* if both $F_k(x)$ and $F_k^{-1}(y)$ have polynomial-time algorithms for all k, x, y.
- A *pseudorandom permutation* is a permutation which cannot be efficiently distinguished from a random permutation, i.e. a permutation uniformly chosen from $\texttt{Perm}_n$.
- A *strong pseudorandom permutation* is a permutation which cannot be efficiently distinguished from a random permutation *even if the distinguisher is given oracle access to the inverse of the permutation.*
- In practice, constructions of strong pseudorandom permutations are called *block ciphers*.

4 Data Encryption Standard (DES)

- DES was proposed by IBM in 1974 in response to a call for proposals from the US National Bureau of Standards (now NIST)
- Adopted as a US federal standard from 1979 to 2005
- In 2000, AES selected as successor to DES.
- DES considered insecure now but still interesting for historical reasons.

4.1 Construction

- Based on the *Feistel transform*
- Let $f : \{0,1\}^n \to \{0,1\}^n$ be any function. The Feistel transform of f is the function $FSTL_f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is defined by

$$FSTL_f(L, R) = (R, f(R) \oplus L)$$

- Even if f is not a bijection, $FSTL_f$ is a bijection.
- The inverse is given by

$$FSTL_f^{-1}(X, Y) = (Y \oplus f(X), X)$$

- DES has a key length of 56 bits and a block length of $n = 64$ bits. It consists of 16 *rounds* of a Feistel transform.
- The 56-bit key K is expanded to a sequence of 16 subkeys $K_1, K_2, \ldots, K_{16}$ each of length 48 bits.
- Decryption uses the same structure as encryption except for the fact that the subkeys are applied in reverse order.
- See pages 41–44 of Bellare-Rogaway notes for full description.

5 References and Additional Reading

- Section 3.5, 3.6 from Katz/Lindell
- Chapter 3 of *Introduction to Modern Cryptography* by Mihir Bellare, Phillip Rogaway, 2005. `http://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf`