Introduction to Modern Cryptography
Exercise Sheet #4

University of Amsterdam, Master of Logic, 2012
Lecturer: Christian Schaffner
TA: Maria Velema

20 November 2012
(to be handed in by Wednesday, 28 November 2012, 11:00)

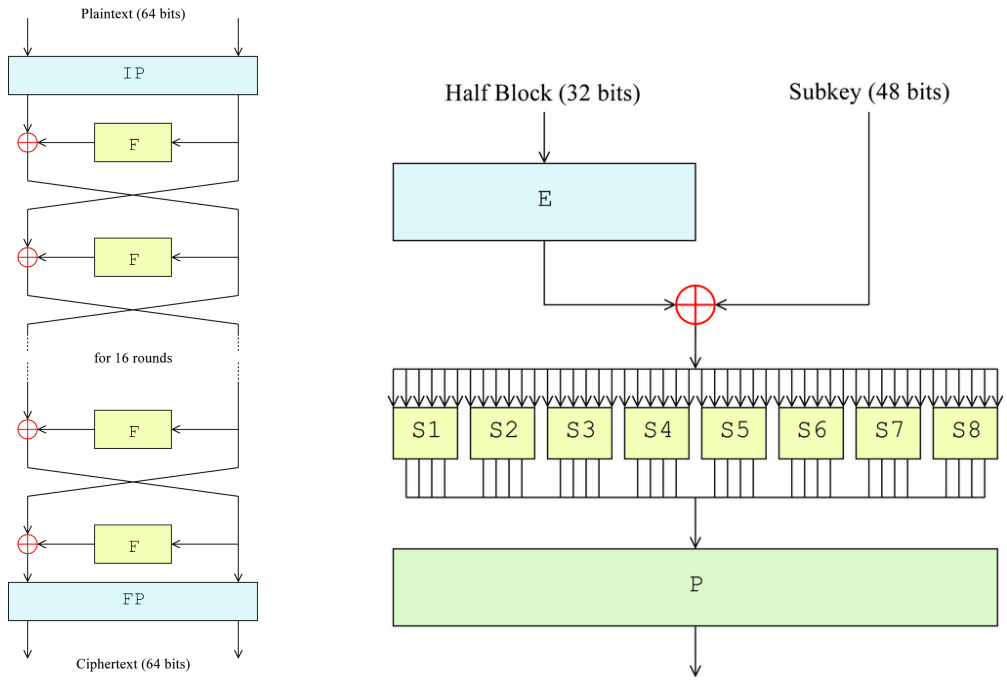
Complementarity Property of DES

In this exercise, we show that DES has the complementarity property, i.e., that $DES_k(x) = \overline{DES_{\overline{k}}(\overline{x})}$ for every key k and input x (where $\overline{z}$ denotes the bitwise complement of z) and how we can exploit that property.

1. Let f be the DES mangler function. Show that for every subkey k and message x, it holds that $f(k,x) = f(\overline{k},\overline{x})$.

2. Use the above property to conclude that after every round i in the Feistel network, $L_i(x,k) = \overline{L_i(\overline{x},\overline{k})}$ and $R_i(x,k) = \overline{R_i(\overline{x},\overline{k})}$. Conclude that $DES_k(x) = \overline{DES_{\overline{k}}(\overline{x})}$ for every key k and input x. (Note that for all "permutations" P in DES, $P(\overline{x}) = \overline{P(x)}$.)

3. Use a chosen-plaintext attack with two messages x and $\overline{x}$ to argue that it is possible to find the secret key in DES (with probability 1) using 2^{55} local computations of DES.



Feistel Network and mangler function of DES
Image credit: `wikimedia.org`.

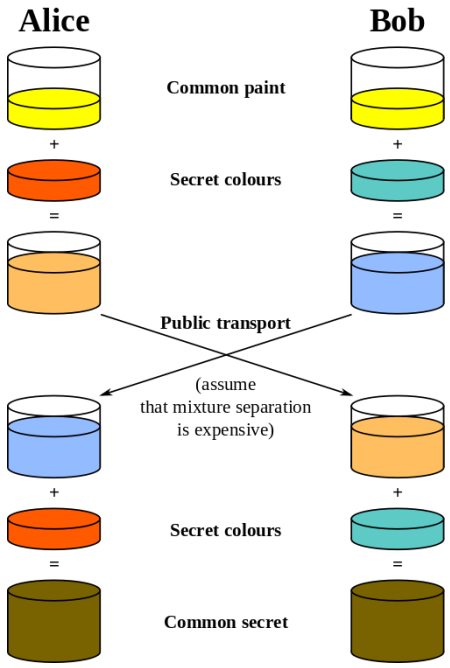
more on the back side

Key Establishment

4. **Interactive Secure Encryption:** Exercise 9.1 in [KL]
5. **Man-In-The-Middle Attacks:** Exercise 9.2 in [KL]
6. **Key Exchange with Bit Strings:** Exercise 9.3 in [KL]
7. **CDH and DDH:**
   (a) Give an example of a (not necessarily multiplicative) group $\mathcal{G}$ relative to which the CDH-Problem is easy.
   (b) Prove formally that the hardness of the CDH problem relative to a group $\mathcal{G}$ implies the hardness of the discrete logarithm problem relative to $\mathcal{G}$. (Exercise 7.15 in [KL])
   (c) Prove formally that the hardness of the DDH problem relative to a group $\mathcal{G}$ implies the hardness of the CDH problem relative go $\mathcal{G}$. (Exercise 7.16 in [KL])

A Good Read

Read and enjoy the paper "New Directions in Cryptography" by Whitfield Diffie and Martin Hellman from November 1976, available from the course webpage.



Diffie-Hellman Key Exchange Using Buckets of Paint
Image credit: `wikimedia.org`.

even more on the next page

Group and (Algorithmic) Number Theory

[Thanks to Boaz Barak for his kind permission to use his exercises.] The following exercises introduce some group and number theory in order to prepare you for the treatment of public-key cryptography.

As mathematicians, we expect you to be able to solve the group theory exercises 8.-12. with ease. **Exercises 8.-12. are optional**: we will correct them (if you decide to hand in solutions), but not grade them. If you are not completely confident in your abilities, we recommend that you hand them in, though. **Exercises 13. and 14. are not optional** and will be graded.

The exercises are self-contained, so you can solve them without reading outside sources. If you want to brush up your knowledge, the following are recommended references: **(1)** [KL], Chapter 7 and Appendix B, **(2)** Victor Shoup's book *"A Computational Introduction to Number Theory and Algebra"* (also available online at `http://www.shoup.net/ntb/`) and **(3)** The mathematical background appendix of the *"Computational Complexity"* book by Sanjeev Arora and Boaz Barak also contains some basic number theory background.

A group $(S, \circ)$ is a set S with a binary operation $\circ$ defined on S for which the following properties hold:

(i) **Closure:** For all $a, b \in S$ it holds that $a \circ b \in S$.

(ii) **Identity:** There is an element $e \in S$ such that $e \circ a = a \circ e = a$ for all $a \in S$.

(iii) **Associativity:** $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in S$.

(iv) **Inverses:** For each $a \in S$ there exists an element $b \in S$ such that $a \circ b = b \circ a = e$.

The order of a group, denoted by $|S|$, is the number of elements in S. If the order of a group is a finite number, the group is said to be a *finite group*. If a group $(S, \circ)$ satisfies the commutative law $a \circ b = b \circ a$ for all $a, b \in S$ then it is called an *Abelian group*.

8. (Optional) Let $+_n$ denote addition modulo n (e.g., $5 +_3 6 = [5 + 6 \mod 3] = 2$). Let $Z_n = \{0, 1, 2, \ldots, n-1\}$. Prove that $(Z_n, +_n)$ is a finite Abelian group for every natural number n.

9. (Optional) Prove that for every group:
   (a) The identity element e in the group is *unique*.
   (b) Every element a has a *single* inverse.

10. (Optional) Let a be an element in a group and let a^{-1} denote the (unique) inverse of a. Then, for every integer k we define:

$$a^k := \begin{cases} \underbrace{a \circ a \circ \ldots \circ a}_{k} & \text{if } k > 0; \\ e & \text{if } k = 0; \\ (a^{-1})^{-k} & \text{if } k < 0. \end{cases}$$

Prove that for any integers m, n (not necessarily positive) it holds that:

(a) $a^m \circ a^n = a^{m+n}$.

(b) $(a^m)^n = a^{mn}$.

11. (Optional) Let $(S, \circ)$ be a group and let $S' \subseteq S$. If $(S', \circ)$ is also a group, then $(S', \circ)$ is called a *subgroup* of $(S, \circ)$. Prove that:

    (a) If $(S, \circ)$ is a finite group and $a \in S$ then there exists $m \geq 1$ such that $a^m = a^{-1}$.

    (b) If $(S, \circ)$ is a finite group and S' is a subset of S such that $a \circ b \in S'$ for every $a, b \in S'$, then $(S', \circ)$ is a subgroup of $(S, \circ)$.

12. (Optional) Let a and b be two positive integers. We denote by $\gcd(a, b)$ the greatest common divisor of a and b; i.e, $d = \gcd(a, b)$ if d is the largest integer that divides both a and b. The *Euclidean algorithm* computes the gcd as follows:

    input: $a > b > 0$
    $r_{-1} \leftarrow a$
    $r_0 \leftarrow b$
    for $i = 1, 2, \ldots$ till $r_i = 0$
        $r_i \leftarrow [r_{i-2} \mod r_{i-1}]$
    output r_{i-1}

    (a) Prove that this algorithm indeed outputs the gcd of a and b.

    (b) Prove that if d is the gcd of a and b, then there exist (not necessarily positive) integers x, y such that $d = xa + yb$. How can you compute these numbers?

13. Let $\times_n$ denote multiplication modulo n (i.e., $5 \times_7 3 = [15 \mod 7] = 1$).

    (a) Prove that for every n, the set $\mathbb{Z}_n^* = \{k \in \{1, \ldots, n-1\} \ ; \ \gcd(k, n) = 1\}$ with the operation $\times_n$ is an Abelian group.

    (b) Give an algorithm that on input $a \in \mathbb{Z}_n^*$, computes a^{-1} (with respect to the group operation $\times_n$). Can you find an algorithm that runs in time polynomial in $|n|$?

    (c) If n is a prime number, how many elements exist in $\mathbb{Z}_n^*$?

    (d) If $n = p \cdot q$ is the product of two different prime numbers p and q, how many elements exist in $\mathbb{Z}_n^*$?

14. **Square-And-Multiply, Efficient Modular Exponentiation:** Exercise B.3 in [KL]. Argue why your algorithm is efficient. **Corrected hint:** Let $y = [a^b \mod N]$ denote the answer. Use auxiliary variables x (initialized to a) and t (initialized to 1), and maintain the invariant $t \cdot x^b = y \mod N$ while decreasing b and squaring x. The algorithm terminates when $b = 0$ and t is equal to the answer.