Cryptography

Prof. Dr. Klaus Meer, Ameen Naif

Exercise Sheet 4
Version 17.05.2018

Exercise 1.

We are given a pair $(p, c) \in \{0,1\}^{64} \times \{0,1\}^{64}$ where c is the encryption of the plaintext p with an unknown key K using 1-Round DES. We want to find the 48-bit key K.

(a) Why is the output of all S-boxes known?

(b) Given the 4-bit output of S_1-Box how many 6-bit combinations are possible as input to S_1-Box?

(c) How many 6-bit combinations are possible as the 6 bit key which takes part in the creation of the input to S_1-Box?

(d) How many 48-bit combinations are possible for K?

Note: the S-boxes, the permutations $\pi \in S_{64}$ and $\sigma \in S_{32}$ and the **expansion function** E in the DES-cryptosystem are fixed and known.

Exercise 2.

Let $n = p \cdot q$ be the product of two unknown prime numbers. Let a, b be two integers such that $e \cdot d = 1 \; mod \; \phi(n)$. Find the prime factors q and p of n in the following cases:

(a) If n and $\phi(n)$ are known.

(b) If n, e and d are known.

Exercise 3.

Let $(G, \cdot)$ be a cyclic group generated by $a \in G$.

(a) Suppose that k is the minimal integers such that $a^l = a^k$ and $l < k$ for some integer l. Then $|G| = n = k - l$ and $G = \{a^0, a^1, ..., a^{n-1}\}$.

(b) Let $m \in \mathbb{N}$ and $d = gcd(m, n)$. Then a^m and a^d generate the same subsets of G.

Exercise 4.

Show the following: If there is a polynomial time decision algorithm for **Factoring II**, then all prime factors of n can be computed in polynomial time. (**Hint**: Binary search for factors of n).

Factoring II: Input $(n, k) \in \mathbb{N}^2$, $k < n$. Question: Is there a factor of n which is $\leq k$?

Exercise 5.

Suppose that **Subset Sum** is $\mathcal{NP}$-complete:

(a) Show that **PARTITION** is in $\mathcal{NP}$.

(b) Prove that **PARTITION** is $\mathcal{NP}$-complete by giving a reduction from **Subset Sum**.

Subset Sum: Input $n, s_1, ..., s_n, T$, all are positive integers. Question: Is there a subset $S \subseteq \{1, ..., n\}$ such that $\sum\limits_{i \in S} s_i = T$

PARTITION: Input $n, s_1, ..., s_n$, all are positive integers. Question: Is there a subset $S \subseteq \{1, ..., n\}$ such that $\sum\limits_{i \in S} s_i = \sum\limits_{i \in \overline{S}} s_i$? Where $\overline{S} = \{1, ..., n\} \setminus S$ is the complement set of S.

Exercise 6.

Let x be a decimal number and suppose that $\log_2 x$ is a positive integer.

i) How can you compute the value $\log_2 x$ efficiently for the input x?

ii) Given a prime p, how can $\log_2 x \ mod \ p$ be computed? What is the running time of your algorithm?