IV054 Coding, Cryptography and Cryptographic Protocols

2008 – Exercises VI.

1. Assume that the ciphertext $c = (512, 303)$ was obtained using the ElGamal cryptosystem with the following parameters: $p = 941$, $q = 2$, $x = 14$ and $r = 9$. Find the plaintext.

2. Consider probability distributions p_0, p_1 over $\{0,1\}^n$ where $n \in \mathbb{N}$. Let A be a polynomial time algorithm with inputs from $\{0,1\}^n$ and outputs from $\{0,1\}$ which has the property

$$Pr(A(p_0) = 1) - Pr(A(p_1) = 1) \geq \epsilon,$$

where $\epsilon > 0$ and $A(p_i)$ denotes the result of a computation of A for an input chosen according to the distribution p_i. Alice and Bob decided to play the following game:

   (a) Alice chooses randomly and uniformly a bit $b \in \{0,1\}$.

   (b) Alice chooses a string x according to the distribution p_b and sends it to Bob.

   (c) Bob returns a bit $b' \in \{0,1\}$.

   (d) Bob wins if $b = b'$.

   Suppose that Bob is able to use the algorithm A. Show that he can win with probability greater than $\frac{1}{2}$.

3. Suppose that an adversary Eve can solve the Diffie-Hellman problem (i.e. given α^x and α^y she can compute α^{xy} (modulo p)). Show that Eve can then easily break the ElGamal encryption scheme.

4. Let $n \in \mathbb{N}$ and $s \in \{0,1\}^n$. Let further $G : \{0,1\}^n \to \{0,1\}^m$ be a pseudo-random generator and $\circ : \{0,1\} \times \{0,1\} \to \{0,1\}$. Finally, let $\circ_n$ be an extension of $\circ$ to bit strings of length n obtained by applying $\circ$ bitwise.

   Consider the encryption scheme with $P = C = \{0,1\}^m$ and $K = \{0,1\}^n$. The encryption e of a message p using a secret key k is defined as $e(p,k) = G(k) \circ_m p$.

   (a) Suppose that $\circ$ is the $\oplus$ operation. Decide whether this encryption scheme is secure against a chosen plaintext attack. Explain your reasoning.

   (b) Is there any other function $\circ' : \{0,1\} \times \{0,1\} \to \{0,1\}$ which can be used as $\circ$? What is its necessary property?

5. Assume that the Shanks' algorithm is used to compute

$$\log_5 71 \pmod{167}.$$

   Show the computation steps.

6. Consider a prime p and an integer $1 < a < p - 1$.
   (a) Suppose that there is n such that $n^2 \equiv a \pmod{p}$. Show that a is not a primitive root $\pmod{p}$.
   (b) Suppose that there is no n such that $n^2 \equiv a \pmod{p}$ and that $\frac{p-1}{2}$ is a prime. Show that a is a primitive root $\pmod{p}$.
7. Let $f(n) = \frac{1}{\binom{2n}{n}}$ and $g(n) = \frac{1}{\binom{n+42}{n}}$. Decide which of these functions is negligible.