Introduction to Cryptography – Exercise no. 3

Submit in Pairs/Single to **mailbox** 19 by 4/5/11, 1:00 p.m.

1. Prof. Menjir has suggested the following compression function: The function accepts a 128-bit chaining value CV and a 1408-bit message block M. The 1408-bit message block M is treated as eleven 128-bit subkeys, i.e., $M = K_0||K_1||\ldots||K_{10}$ (the first 128-bit of the message being the first subkey, etc.). To compress the inputs, the value CV is encrypted using 10 rounds of AES, where the 11 subkeys are $K_0, K_1, \ldots, K_{10}$, with an additional feed-forward.

   Formally:
   $$CV' = AES_{K_0,K_1,\ldots,K_{10}}(CV) \oplus CV.$$

   (a) Show how to construct collisions in this compression function as efficiently as you can.

   (b) Show how to find a preimage of a given chaining value in this hash function as efficiently as you can.

2. Calculate by using the Euclidean Algorithm:

   (a) $\gcd(770, 882)$

   (b) $\gcd(975, 572)$

   (c) The inverse of 48 modulo 137.

   (d) The inverse of 20 modulo 137.

   Provide the steps of the computation in your answers.

3. This question deals with the complexity of the Euclidean Algorithm. Assume that we start the algorithm with $a > b > 0$ and we get:

$$\begin{array}{lcll} a & = & q_1 b + r_1 & 0 < r_1 < b \\ b & = & q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & q_3 r_2 + r_3 & 0 < r_3 < r_3 \\ \vdots & & & \\ r_{n_2} & = & q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n_1} & = & q_{n+1} r_n & \end{array}$$

   Denote $\alpha = \frac{1+\sqrt{5}}{2} \approx 1.618$.

   (a) Prove that $\alpha^2 = \alpha + 1$.

   (b) Prove that $r_{n-i} \geq \alpha^i$ for all $0 \leq i < n$.

   (c) Prove that the number of divisions in the Euclidean Algorithm $\leq \log_\alpha a$.

   (d) Is this bound tight?

4. Solve the following two systems:

$$\begin{cases} x \equiv 2 & (\text{mod } 5) \\ x \equiv 3 & (\text{mod } 7) \\ x \equiv 4 & (\text{mod } 11) \end{cases}$$

and

$$\begin{cases} x \equiv 2 & (\text{mod } 4) \\ x \equiv 4 & (\text{mod } 6) \\ x \equiv 8 & (\text{mod } 13) \end{cases}$$

Describe the steps you have used in your solution.

5. Let p be a prime number and assume that the decomposition of $p-1$ into its prime factors is known.

   (a) Show an algorithm that given a number $g \in Z_p^*$ can determine whether g is a generator of Z_p^*. Analyze the time complexity of the algorithm you suggested, and prove its correctness (Algorithms that require more than $O(log^3(p))$ modular multiplications will be disregarded).

   (b) Show an algorithm that given a number $g \in Z_p^*$ can find the order of g in Z_p^* . Your algorithm should not perform more than $O(log3(p))$ modular multiplications. Analyze the time complexity of the algorithm you suggested.

6. In this question, you are requested to compute a Diffie-Hellman key. For this purpose, we shall use $p = 44449$ and $g = 11114$.

   Usually, one first selects the secret keys, and then the public keys are computed. However, we shall start by selecting the public keys, which then will be used to compute the secret keys, and then the joint key.

   Let y_1 be digits 2–5 of the ID of the first submitter, i.e., if your ID is 123456789, $y_1 = 2345$. Let y_2 be digits 6–9 of the ID of the second submitter (unless there is one, and then these are the digits of the ID number of the submitter).

   (a) Find x_1 for which $g^{x_1} \equiv y_1 \bmod p$ and x_2 for which $g^{x_2} \equiv y_2 \bmod p$.

   (b) Compute the Diffie-Hellman key produced by the public keys y_1, y_2.

   (c) Given the public key $y = 23893$, find its corresponding x. Explain how you succeeded to do so, despite the fact that Diffie-Hellman is secure.