VE475
Introduction to Cryptography

Assignment 6 (06/07/2017)

Manuel — UM-JI (Summer 2017)

Non-programming exercises:
- Write in a neat and legible handwriting, or use LaTeX
- Clearly explain the reasoning process
- Write in a complete style (subject, verb and object)

Progamming exercises:
- Write a README file for each program
- Upload an archive with all the programs onto Sakai

Ex. 1 — *Application of the the DLP*

Bob wants to prove his identity to Alice. Alice knows that Bob can compute $\log_\alpha \beta$ in $\mathbb{Z}/p\mathbb{Z}$, where α is a generator of the group $\mathbb{Z}/p\mathbb{Z}$, and p is a known prime. Unfortunately Bob is not willing to share the result with her, so he offers to apply the following strategy.

(i) Bob generates a random integer r and sends $\gamma = \alpha^r \bmod p$ to Alice;
(ii) Upon receiving γ Alice randomly requests r or $x + r \bmod (p-1)$;
(iii) Bob replies accordingly;

We now want to study Bod's idea.

1. In the previous protocol,
   a) Why are r and $x + r$ considered modulo $(p-1)$?
   b) Prove that neither Bob nor Alice can cheat, while Bob can successfully prove his identity.
2. How many times should this be repeated for a
   a) 128 bits security level?
   b) 256 bits security level?
3. What type of protocol is this?

Ex. 2 — *Pohlig-Hellman*

Search and explain in details how the Pohlig-Hellman algorithm computes the discrete logarithm of an element in a multiplicative group whose order can be completely factorized into small primes. As an example calculate $\log_3 3344$ in $G = \mathsf{U}(\mathbb{Z}/24389\mathbb{Z})$, knowing that 3 is generator of G.

Ex. 3 — *Elgamal*

1. Prove that the polynomial $X^3 + 2X^2 + 1$ is irreducible over $\mathbb{F}_3[x]$, and conclude that it defines the field $\mathbb{F}_{3^3}$, which has 27 elements.
2. Explain how to define a simple map from the set of the letters of the alphabet into $\mathbb{F}_{3^3}$.
3. What is the order of the subgroup generated by X?
4. If we set the ecret key to be 11, determine the public key.
5. Encrypt the message "goodmorning", and then decrypt the ciphertext.

Ex. 4 — *Simple questions*

1. Let n be the product two large primes, p and q. We define $h(x) \equiv x^2 \bmod n$. Is h (i) pre-image resistant, (ii) second pre-image resistant, and (iii) collision resistant?
2. Supposed a message m is divided into blocks of 160 bits: $m = m_1 \| m_2 \| \cdots \| m_l$. Which properties of a hash function does the function $h(m) = m_1 \oplus m_2 \oplus \cdots \oplus m_l$ verify?

Ex. 5 — *Merkle-Damgård construction*

The Merkle-Damgård construction provided in the slides is only valid when $t \leq 2$, therefore we now use the same notations as in the slides to provide an alternative construction for $t = 1$.

Let g be a compression function from $\{0,1\}^{m+1} \longrightarrow \{0,1\}^m$, and f be the function defined by $f(0) = 0$ and $f(1) = 01$. The map from x to y is defined by $y = 11\|f(x_1)\|f(x_2)\|\ldots\|f(x_{|x|})$, where x_i represents the i-th bit of x. Assuming $|y| = k$, compute

$$\begin{cases} z_1 = g(0^m\|y_1) \\ z_{i+1} = g(z_i\|y_{i+1}), \quad 1 \leq i \leq k-1, \end{cases}$$

and define $h(x)$ as z_k.

1. Check that
   a) The map s from x to y is injective.
   b) There is no strings $x \neq x'$ and z such that $s(x) = z\|s(x')$.
2. Explain why the two previous conditions are of a major importance.
3. Following a similar strategy as in the case $t \geq 2$, prove that h is a collision resistant hash function.

Ex. 6 — *Programming*

Implement the Pollard-rho factorization algorithm.