VE475

Introduction to Cryptography

Assignment 8 (24/07/2017)

Manuel — UM-JI (Summer 2017)

Non-programing 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 — *Lamport one-time signature scheme*

1. Describe the Lamport signature scheme.
2. Highlight the benefits and drawbacks of this method.
3. Explain how this scheme can be attacked is a same key is used to sign more than one message.
4. What is a *Merkle tree*, and how can it be used to improve the efficiency of the Lamport one-time signature scheme?

Ex. 2 — *Chaum-van Antwerpen signatures*

In the lectures we presented the concept of undeniable signatures but we did not prove any of the results. We now do it, reusing the same notations.

1. In this question we want to prove that if $s \not\equiv m^x \bmod p$, then s will be accepted as a valid signature with probability less than $1/q$.
   a) For each value r Alice generates, how many ordered pairs $\langle e_1, e_2 \rangle$ can be considered?
   b) Writing $r = \alpha^i$, $t = \alpha^j$, $m = \alpha^k$, and $s = \alpha^l$, $i, j, k, l \in \mathbb{Z}/q\mathbb{Z}$, consider the system of congruences
   $$\begin{cases} r & \equiv s^{e_1}\beta^{e_2} \bmod p \\ t & \equiv m^{e_1}\alpha^{e_2} \bmod p, \end{cases}$$
   and prove it has a unique solution.
   c) Conclude on the probability that Alice accepts an invalid signature.
2. We now prove that if $s \not\equiv m^x \bmod p$, and the disavowal protocol is respected then we should have $\left(t_1\alpha^{-e_2}\right)^{f_1} \equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \bmod p$.
   a) Prove that
   $$\left(t_1\alpha^{-e_2}\right)^{f_1} \equiv s^{e_1 f_1 x^{-1}} \bmod p.$$
   b) Applying the same method to $\left(t_2\alpha^{-f_2}\right)^{e_1} \bmod p$ conclude that Bob can convince Alice that an invalid signature is a forgery.
3. We finally prove that if $s \equiv m^x \bmod p$, but $t_1 \not\equiv m^{e_1}\alpha^{e_2}$ and $t_2 \not\equiv m^{f_1}\alpha^{f_2}$, then $\left(t_1\alpha^{-e_2}\right)^{f_1} \not\equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \bmod p$ with probability $1 - 1/q$.
   a) Prove this result by contradiction using question 1.
   b) Does this result require Bob to follow the disavowal protocol?
   c) Can Bob convince Alice that a valid signature is a forgery?

Ex. 3 — *Simple questions*

1. DSA with the parameters $q = 101$, $p = 7879$, $\alpha = 170$, $x = 75$, and $\beta = 4567$ is used to signed a message whose hash is 52.
   a) Determine the signature of the message if $k = 49$.
   b) Verify the signature.
2. Bob used the Elgamal signature scheme to sign his messages $m_1 = 8990$ and $m_2 = 31415$. He got $\langle m1, 23972, 31396\rangle$, and $\langle m_2, 23972.20481\rangle$. Knowing his public parameters are $p = 31847$, $\alpha = 5$, and $\beta = 25703$, recover both the random value k and his private key x.