Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 24
October 29, 1998

Solutions to Problem Set 5

Problem 5-1. ElGamal Signature Variant

There were two popular approaches to the question. One results in an insecure scheme ($s' = \frac{M-r}{k}$). The other involves requiring that x is selected such that $gcd(x, p-1) = 1$, and then letting

$$s' = \frac{M - rx}{xk}$$

Demonstrating the insecurity of the former was easy (simply show how to generate unlimited valid signatures). The security of the latter was harder to prove, but demonstrated that in order to provide a forgery, one would need to solve the discrete log problem to get x, which is used in the equation and is directly related to s and y.

Problem 5-2. DSA needs good random bits

Hristo Bojinov
Jordan Gruevski
Valentin Spitkovsky
Svetoslav Tzvetkov

In the solution we work only modulo q (and all equations are modulo q). Therefore, every non-zero number is invertible. We will use $m_1 = H(M_1)$ and $m_2 = H(M_2)$. First we must note that after q signatures it becomes t rivial to recover the key x. However, this is not practical because having in mind the size of q we could no t expect Alice to use her signature q times in her life. We will only need a few (2-4) consequent signed messa ges in order to break the secret key.

(a)

For the solution we only need two consequent signed messages. We have:

$$k^{-1}(m_1 + xr_1) = s_1 \pmod q \tag{1}$$

$$(k+1)^{-1}(m_2 + xr_2) = s_2 \pmod q \tag{2}$$

From (1) and (2) we can express k in terms of x:

$$k = (m_1 - r_1 x)s_1^{-1} \pmod q$$

$$k = (m_2 - r_2 x)s_2^{-1} \pmod q$$

We can now solve for x:

$$x = (m_2 s_1 - s_1 s_2 - m_1 s_2)(s_1 r_2 - s_2 r_1)^{-1}$$

The only thing we need to cover yet is the case when one of the expression we invert above is actually zero. Eve n if that is possible, we can get another pair of signatures and use them to find x. It would be extremely unl ikely to get a zero again. If we keep on getting pairs of signatures such that $s_1 r_2 - s_2 r_1 = 0$ this would mean that there is a big problem with DSA...

(b)

This is very similar to (a):

$$k^{-1}(m_1 + xr_1) = s_1 \pmod q \tag{3}$$
$$(2k)^{-1}(m_2 + xr_2) = s_2 \pmod q \tag{4}$$

By exactly the same manipulations we get:

$$x = (m_2 s_1 - 2m_1 s_2)(r_2 s_1 - 2s_2 r_1)^{-1}$$

(c)

The problem here is a little bit more complicated because we do not know a and b. If we try to solve it acco rding to the addendum (i.e. with $k_i = ak_{i-1} + b$), we can get 4 consequent signed messages and solve for k, x, a and b. However we will need to solve equations of order 3 (i.e. with terms like a^3). We will show how to do this as was originally required in the problem set. Namely, we assume that $k_i = ai + b$. We then have:

$$k^{-1}(m_1 + xr_1) = c_1 \pmod q \tag{5}$$
$$(k + a)^{-1}(m_2 + xr_2) = c_2 \pmod q \tag{6}$$
$$(k + 2a)^{-1}(m_3 + xr_3) = c_3 \pmod q \tag{7}$$

From (5) it follows that $k = (m_1 + xr_1)c_1^{-1}$. We substitute in (6) and (7):

$$(m_2 + xr_2) = c_2 a + c_2 c_1^{-1}(m_1 + xr_1)$$

$$(m_3 + xr_3) = 2c_3 a + c_3 c_1^{-1}(m_1 + xr_1)$$

Therefore $a = ((m_2 - c_2 c_1^{-1} m_1) + (r_2 - c_2 c_1^{-1} r_1)x)c_2^{-1}$. We can now substitute a in one of the last two equalities to get x.

(d)

The smart card Alice bought could have a specific algorithm for generating k's which enables the accomplice to discover Alice's key. For example, an algorithm like the one in the previous sections would suffice. It could b e made slightly more complicated, so that it is not obvious how each k_i is generated (for example k_i could be random for $i = 0 \pmod 3$) and equal to $ak_{i-1} + b$ otherwise). In this way it will not be very obvious that the card is leaking the secret key, but it will be almost as easy to find x.

Problem 5-3. Intentionally weak keys

There is no "right" answer to this problem. Any solution that demonstrated an understanding of the problem, and a good analysis of a solution got credit.