Dr. Michael Reyer

Tutorial 8
- Proposed Solution -

Friday, December 21, 2018

Solution of Problem 1

Parameters: $n = p\,q$ with $p, q \equiv 3 \pmod 4$, and p, q secret primes.
Each user chooses an arbitrary sequence of seeds $s_1, \dots, s_K \in \{1, \dots, n-1\}$, with $\gcd(s_i, n) = 1$ and publishes: $v_i = (s_i^2)^{-1} \mod n$.

A public hash function is applied:

$$h : \{0,1\}^* \to \{0,1\}^K$$

Signature generation:

(i) A chooses an arbitrary value $r \in \{1, \dots, n-1\}$ and calculates $x = r^2 \mod n$. (witness)

(ii) A calculates: $(b_1, \dots, b_k) = h(m, x)$ (challenge)
and afterwards $y = r \prod_{j=1}^{K} s_j^{b_j} \mod n$ (response)

(iii) The signature of m is (x, y):
$A \to B : m, x, y$

Verification:

(i) B calculates $(b_1, \dots, b_K) = h(m, x)$. (challenge)

(ii) B calculates $z = y^2 \prod_{j=1}^{K} v_j^{b_j} \mod n$. (response)

(iii) B accepts the signature if $z = x$ holds.

Proof that this signature and verification scheme is correct:

$$z = y^2 \prod_{j=1}^{K} v_j^{b_j} \equiv \underbrace{r^2}_{\equiv x} \underbrace{\prod_{j=1}^{K} s_j^{2b_j} \prod_{j=1}^{K} v_j^{b_j}}_{\equiv 1} \equiv x \pmod n. \blacksquare$$

Solution of Problem 2

a) The secret service (MI5) chooses an arbitrary seed $s \in \mathbb{Z}_n$ per iteration.

The MI5 calculates the quadratic residue $y = s^2 \mod n$:

MI5 $\to$ JB: y

JB calculates the four square roots of y modulo n using the factors p, q of n.
JB chooses a square root x:

JB $\to$ MI5: x

The MI5 verifies that $x^2 \equiv y \pmod{n}$.

Since JB has no information about s, he chooses the x with probability $\frac{1}{2}$, such that $x \not\equiv \pm s \pmod{n}$.
If the MI5 receives such an x, n can be factorized:

$$\begin{aligned} y \equiv s^2 \equiv x^2 \pmod{n} \\ \Rightarrow s^2 - x^2 \equiv 0 \pmod{n} \\ \Rightarrow (s-x)(s+x) \equiv 0 \pmod{n}. \end{aligned}$$

The probability that JB always fails by sending $x \equiv \pm s \mod n$ in all 20 submissions is:

$$\tfrac{1}{2^{20}} = \tfrac{1}{1048576} \approx 10^{-6}.$$

b) *Zero-knowledge property:* No information about the secret may be revealed during the response.

However, in this protocol it is even possible, that the full secret s is revealed. Hence, this is not a secure zero-knowledge protocol!

c) A passive eavesdropper E can only obtain the values x and y. E only knows the square roots $\pm x$ of y modulo n, which is useless in the next iteration. This knowledge is not sufficient to factorize n. Obviously, the MI5 should not use the same y twice.

Solution of Problem 3

a) O knows y. He needs to send a pair (x_1, x_2) with $x_1 \cdot x_2 \equiv y \pmod{n}$ to B. Then B will ask O to provide a square root of either x_1 or x_2. If O is able to give the square roots for both x_1 and x_2, he can compute a square root of y which is infeasible. Hence, O may know at most one square root. O chooses a random number s_1 computes the numbers $x_1 = s_1^2 \mod n$ and $x_2 = yx_1^{-2} \mod n$ and sends (x_1, x_2) to B. O may calculate the square root of x_1 as s_1 but cannot do so for x_2 and hence has a 50% chance of giving the right answer. Note that x_1 needs to be invertible modulo n. If this is not the case then O has been lucky and is able to factorize n and break the system.

b) As the success probabilty for O is 0.5, O need to ask 10 times as $2^{10} = 1024 > 10^3$.

c) If B does not check $x_1 \cdot x_2 \mod n = y$, O may send $(x_1, x_2) = (s_1^2 \mod n, s_2^2 \mod n)$.

d) If A uses the same random number r_1 more than once O (as well as B) could get square roots of x_1 and x_2 and hence a square root of y. Particularly, B could directly ask for the other square root in the second time using the same r_1.

e) If r_1 is not repeated, O cannot learn from listening to the protocol as he only learns abut one square root. If he is asked for the second square root O is lost as above.