Prof. Dr. Rudolf Mathar, Dr. Michael Reyer, Jose Leon, Qinwei He

Exercise 6
- Proposed Solution -

Friday, December 1, 2017

Solution of Problem 1

Recall for **a)**, **b)** and **c)** that we have: $r = a^k \mod p$ and $y = a^x \mod p$ from the ElGamal signature scheme.

a) This is easily solved by substituting $s = x^{-1}(h(m) - kr)$, r and y:

$$\begin{aligned} v_1 \equiv y^s r^r &\equiv y^{x^{-1}(h(m)-kr)} a^{kr} \\ &\equiv a^{xx^{-1}(h(m)-kr)} a^{kr} \\ &\equiv a^{(h(m)-kr)+kr} \\ &\equiv a^{h(m)} \equiv v_2 \mod p. \end{aligned}$$

If the given signature is properly checked, $v_1 = y^s r^r = a^{h(m)} = v_2 \mod p$ is true.

b) In this case it is useful to proceed stepwise. We begin with computing:

$$a^s \equiv a^{xh(m)+kr} \equiv a^{xh(m)} a^{kr} \mod p.$$

Next, we substitute y and r, correspondingly, and we rearrange the congruence:

$$\begin{aligned} a^s &\equiv y^{h(m)} r^r \mod p \\ \Leftrightarrow a^s r^{-r} &\equiv y^{h(m)} \mod p. \end{aligned}$$

In the last step, we fix the parameters for verification by:

$$\begin{aligned} v_1 &\equiv a^s r^{-r} \mod p, \\ v_2 &\equiv y^{h(m)} \mod p, \end{aligned}$$

so that $v_1 = v_2$ must be checked by the proposed scheme.

c) In analogy to **b)**, we compute:

$$\begin{aligned} a^s &\equiv a^{xr+kh(m)} \\ &\equiv a^{xr} a^{kh(m)} \\ &\equiv y^r r^{h(m)} \mod p \\ \Leftrightarrow v_1 = a^s y^{-r} &\equiv r^{h(m)} = v_2 \mod p. \end{aligned}$$

Solution of Problem 2

We have a generator $a \equiv g^{\frac{p-1}{q}} \mod p$, with $g \in \mathbb{Z}_p^*$, $q \mid p-1$, p, q prime and $a \neq 1$. By definition of the order of a group, we know that:

$$a^{\mathrm{ord}_p(a)} \equiv 1 \mod p.$$

Recall: $\mathrm{ord}_p(a) = \min\{k \in \{1, ..., \varphi(p)\} \mid a^k \equiv 1 \mod p\}$. With $a \neq 1 \to \mathrm{ord}_p(a) > 1$. Next, we compute a^q and substitute $g^{\frac{p-1}{q}}$:

$$a^q \equiv \left(g^{\frac{p-1}{q}}\right)^q \equiv g^{p-1} \overset{\text{Fermat}}{\equiv} 1 \mod p.$$

From this we obtain $1 < \mathrm{ord}_p(a) \leq q$.

Yet to show: Does a $k \in \mathbb{Z}$ with $k < q$ exist so that k is the order of the group?

This is a proof by contradiction.

Assume the subgroup has indeed $k = \mathrm{ord}_p(a) < q$, i.e., $\exists k < q : k = \mathrm{ord}_p(a)$. Then:

$$\begin{aligned} a^q &\equiv a^{lk+r}, \;\; l \in \mathbb{Z}, r < k, \\ &\equiv a^r \\ &\overset{!}{\equiv} 1 \mod p. \end{aligned}$$

We distinguish two possible cases:

- $\mathrm{ord}_p(a) \nmid q \Rightarrow a^r \equiv 1 \mod p$, with $1 < r < \mathrm{ord}_p(a)$ ↯ (Def. of $\mathrm{ord}_p(a)$)
- $\mathrm{ord}_p(a) \mid q \Rightarrow a^0 \equiv 1 \mod p$ ✓

Since q is prime $\Rightarrow \mathrm{ord}_p(a) \mid q$ there are only two divisors of q, namely 1 and q:

- $\mathrm{ord}_p(a) = 1$ ↯ (since $a \neq 1$ is assumed)
- or $\mathrm{ord}_p(a) = q$ ↯ (We obtain $k = q$ and not the demanded $k < q$)

The cyclic subgroup has order q in $\mathbb{Z}_p^*$, if a is chosen according to the algorithm.

Solution of Problem 3

Choose a pair $(\tilde{u}, \tilde{v}) \in \mathbb{Z} \times \mathbb{Z}$ such that $\gcd(\tilde{v}, q) = 1$, so that $\tilde{v}$ is invertible modulo q.

The forged signature is constructed by:

$$r \equiv (a^{\tilde{u}} y^{\tilde{v}} \mod p) \mod q,$$
$$s \equiv r\tilde{v}^{-1} \mod q,$$

Then (r, s) is a valid signature for the message $m = s\tilde{u} \mod q$.

Check verification procedure of the DSA:

1. Check $0 < r < q$, $0 < s < q$. ✓ (due to modulo q)
2. Compute $w \equiv s^{-1} \mod q$.
3. In this step, no hash-function is used by the given assumption, i.e., $h(m) = m$:
   $u_1 \equiv wm \equiv s^{-1}s\tilde{u} \equiv \tilde{u} \mod q$,
   $u_2 \equiv rw \equiv rs^{-1} \mod q$.
4. $v = a^{u_1} y^{u_2} \equiv a^{\tilde{u}+xrs^{-1}} \equiv a^{\tilde{u}+\tilde{v}x} \equiv a^{\tilde{u}}(a^x)^{\tilde{v}} \equiv (a^{\tilde{u}} y^{\tilde{v}} \mod p) \mod q$.
5. The forged DSA signature is valid, since $v = r$ holds. ✓

Solution of Problem 4

a) We demand the following conditions on the two prime parameters p and q:

i) $2^{159} < q < 2^{160}$,
ii) $2^{1023} < p < 2^{1024}$,
iii) $q \mid p - 1$.

We use a stepwise approach going through i), ii), and iii).

Our suggested algorithm to find a pair of primes p and q is:

1) Get a random *odd* number q with $2^{159} < q < 2^{160}$.
2) Repeat step 1) if q is not prime. (e.g., use the Miller-Rabin Primality Test)
3) Get a random *even* number k with $\left\lceil \frac{2^{1023}-1}{q} \right\rceil < k < \left\lfloor \frac{2^{1024}-1}{q} \right\rfloor$ and set $p = kq + 1$.
4) If p is not prime, repeat step 3).

Check if the algorithm finds a correct pair of primes p, q according to i), ii), and iii):

- With step 1), $2^{159} < q < 2^{160}$ holds, as demanded in i). ✓
- Due to step 2), q is prime. ✓
- Due to step 3), it holds:

$$p = kq + 1 \overset{ii)}{>} \left\lceil \frac{2^{1023}-1}{q} \right\rceil q + 1 \geq 2^{1023},$$
$$p = kq + 1 \overset{ii)}{<} \left\lfloor \frac{2^{1024}-1}{q} \right\rfloor q + 1 \leq 2^{1024},$$

  and therefore $2^{1023} < p < 2^{1024}$ holds, as demanded in ii). ✓

- Step 3) also provides $p = kq + 1 \Leftrightarrow q \mid p - 1$, as demanded in iii).
  An *even* k ensures that p is an odd number.
- Step 4) provides that p is also prime.

Altogether, the proposed algorithm works.

b) In steps 2) and 4), a primality test is chosen (here: Miller-Rabin Primality Test), such that the error probability for a composite q is negligible.

The success probability of finding a prime of size x is about $\frac{1}{\ln(x)}$. (cf. hint)

If even numbers (these are obviously not prime) are skipped, the success probability doubles. The success probability of finding a single prime is estimated by:

$$p_{\text{succ},p} \approx 2 \cdot \frac{|\{p \in \mathbb{Z} | p \leq n,\ p \text{ prime }\}|}{n}.$$

The combined probability of success for a pair of primes p and q is approximately:

$$= \frac{2}{\ln(2^{160})} \cdot \frac{2}{\ln(2^{1024})} = \frac{1}{80 \cdot 512 \cdot \ln(2)^2} \approx 5.08 \cdot 10^{-5}.$$