

Dr. Michael Reyer

Tutorial 6

- Proposed Solution -

Friday, November 30, 2018

Solution of Problem 1

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

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

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

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

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

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

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

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

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

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

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

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

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

Solution of Problem 2

We have a generator $a \equiv g^{\frac{p-1}{q}} \pmod{p}$, 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:

$$a^{\text{ord}_p(a)} \equiv 1 \pmod{p}.$$

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

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

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

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 $k = \text{ord}_p(a) < q$, i.e., $\exists k < q : k = \text{ord}_p(a)$. Then:

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

We distinguish two possible cases:

- $\text{ord}_p(a) \nmid q \Rightarrow a^r \equiv 1 \pmod{p}$, with $1 < r < \text{ord}_p(a) \nmid$ (Def. of $\text{ord}_p(a)$)
- $\text{ord}_p(a) \mid q \Rightarrow a^0 \equiv 1 \pmod{p} \checkmark$

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

- $\text{ord}_p(a) = 1 \nmid$ (since $a \neq 1$ is assumed)
- or $\text{ord}_p(a) = q \nmid$ (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 $(\tilde{u}, \tilde{v}) \in \mathbb{Z} \times \mathbb{Z}_q^*$.

The forged signature is constructed by:

$$\begin{aligned} r &= (a^{\tilde{u}} y^{\tilde{v}} \pmod{p}) \pmod{q}, \\ s &= r \tilde{v}^{-1} \pmod{q}, \end{aligned}$$

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

Check verification procedure of the DSA:

1. Check $0 < r < q$, $0 < s < q$. \checkmark (due to modulo q)

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

$$p = kq + 1 \stackrel{ii)}{>} \left\lceil \frac{2^{1023}-1}{q} \right\rceil q + 1 \geq 2^{1023},$$

$$p = kq + 1 \stackrel{ii)}{<} \left\lfloor \frac{2^{1024}-1}{q} \right\rfloor q + 1 \leq 2^{1024},$$

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:

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

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

$$= \frac{2}{\ln(2^{160})} \cdot \frac{2}{\ln(2^{1024})} = \frac{1}{80.512 \cdot \ln(2)^2} \approx 5.08 \cdot 10^{-5}.$$