Exercise 11 in Cryptography - Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo
2015-07-16

Solution of Problem 36

a) Show that the Babystep-Giantstep-Algorithm computes the discrete logarithm.

$$\begin{aligned} b_j &= \alpha^j \mod p, \\ g_i &= \beta\alpha^{-im} \mod p, \\ x &\equiv j + im \mod p-1 \end{aligned}$$

The equation $b_j \equiv g_i$ yields:

$$\begin{aligned} \alpha^j &\equiv \beta\alpha^{-im} \mod p \\ \alpha^{j+im} &\equiv \beta \mod p \\ \alpha^x &\equiv \beta \mod p \end{aligned}$$

b) a being a primitive element of the group $\mathbb{Z}_p^*$ means, all elements in the group $\beta \in \mathbb{Z}_p^*$ have a representation as $a^n \mod p, n \in \{0, \dots, p-1\}$. This guarantees existence and uniqueness in the output of the algorithm.

Take for example $a = 1$, which is obviously no primitive element. Then, $b_j = 1 \, \forall j$ and $g_i = \beta \, \forall i$. No value $\beta \neq 1$ has a solution for n. $\beta = 1$ is the only possible value, but the solution for n is not unique.

c) $\alpha^x \equiv \beta \mod p$, $\alpha = 3$, $p = 29$, $\beta = 13$.

Task: Compute $x = \log_\alpha(\beta)$ using the Babystep-Giantstep-Algorithm.

(1) $m = \lceil 29 \rceil = 6$

i/j	0	1	2	3	4	5
(2) $b_j = \alpha^j \mod p$	1	3	9	27	23	11
(3) $g_i = \beta\alpha^{-im} \mod p$	13	25	28	7	9	24

Note that $\alpha^{-1} \equiv 10 \mod p$, since $3 \cdot 10 - 1 \cdot 29 = 1 \Rightarrow \alpha^{-m} \equiv 10^6 \equiv 22 \mod 29$.

(4) For $(j, i) = (2, 4) \Rightarrow b_2 = g_4 = 9$ holds

$$\begin{aligned} x &= mi + j \mod (p-1) \\ &\equiv 6 \cdot 4 + 2 \mod 28 \\ &\equiv 26 \mod 28 \end{aligned}$$

The discrete logarithm is $x = 26$.
(Check: $3^{26} = 3^{13}3^{13} \equiv 19 \cdot 19 \equiv 13 \mod 29$)

Remark on complexity:

Running: $2\sqrt{p} \approx \mathcal{O}(\sqrt{p})$

Bruteforce: $\mathcal{O}(p)$

Solution of Problem 37

As given, we have the parameters $a, b \in \mathbb{Z}$ and $a', b' \in \mathbb{Z}$. Furthermore, we have $M = ab - 1$, the private key $d = b'M + b$, and the public key (n, e) with $e = a'M + a$, and $n = \frac{ed-1}{M}$. By substitution we obtain the following for n:

$$\begin{aligned} n &= \frac{ed-1}{M} \\ &= \frac{(a'M+a)(b'M+b)-1}{M} \\ &= \frac{a'b'M^2 + a'bM + ab'M + ab - 1}{M} \\ &= a'b'M + a'b + ab' + 1. \end{aligned}$$

a) The encryption operation is computing $c \equiv em \mod n$. The decryption operation is computing $dc \mod n$. From $dc \equiv dem \mod n \overset{!}{\equiv} m \mod n$, it follows that $de \equiv 1 \mod n$ must hold:

$$\begin{aligned} de &\equiv (a'M+a)(b'M+b) \mod n \\ &\equiv a'b'M^2 + ab'M + a'bM + ab \mod (a'b'M + ab' + ba' + 1) \\ &\equiv 1 \mod (a'b'M + ab' + ba' + 1). \end{aligned}$$

For the given system, $de \equiv 1 \mod n$ is always true.

b) We consider an attack to break the private key d. Note that c, n, e are public. Furthermore, since $de \equiv 1 \mod n$ holds, it follows that $\gcd(de, n) = 1$. We can compute the inverse of e modulo n using the Euclidean algorithm. As $e^{-1} \equiv d \mod n$ holds, the private key is easily computed using the Euclidean algorithm.

Solution of Problem 38

a) The parameters of the given ElGamal cryptosystem are $p = 3571$, $a = 2$, $y = 2905$.

1) Check whether p is prime: Yes, use the MRPT in general or the exaustive search in this simple case. Since $\sqrt{3571} > 59$ it suffices to perform trial division for all primes less or equal to 59.
2) Check whether a is a primitive element modulo p:

$$a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p}, \ \forall i = 1, \dots, k,$$

with the prime factorization $p - 1 = \prod_{i=1}^{k} p_i^{t_i}$ as given in Proposition 7.5.

The prime factorization yields: $3570 = 2{\cdot}1785 = 2{\cdot}5{\cdot}357 = 2{\cdot}5{\cdot}17{\cdot}21 = p_1p_2p_3p_4$.

$$\begin{aligned} p_1 = 2: &\ 2^{1785} \pmod p \equiv -1, \\ p_2 = 5: &\ 2^{714} \pmod p \equiv 2910, \\ p_3 = 17: &\ 2^{210} \pmod p \equiv 1847, \\ p_4 = 21: &\ 2^{170} \pmod p \equiv 2141. \end{aligned}$$

a is a primitive element modulo p.

b) The first part of both ciphertexts is equal. Bob has chosen the same session key twice.

c) One message $m_1 = 567$ is given. We perform a known-plaintext attack.

Let $\boldsymbol{c}_1 = (c_1, c_2)$ and $\boldsymbol{c}_2 = (c_3, c_4)$.

The session key k is the same, since the ciphertexts c_1 and c_3 are congruent:

$$c_1 \equiv c_3 \equiv a^k \pmod p.$$

With $y = a^x \pmod p$, K is computed by:

$$K = y^k \equiv a^{xk} \mod p,$$

in both cases.

For the known m_1, c_2 and p we can compute K^{-1}:

$$\begin{aligned} m_1 &\equiv K^{-1}c_2 \pmod p \\ \Leftrightarrow K^{-1} &\equiv c_2^{-1}m_1 \pmod p, \end{aligned}$$

and finally reveal m_2:

$$\begin{aligned} m_2 &\equiv c_4K^{-1} \pmod p \\ &\equiv c_4c_2^{-1}m_1 \pmod p. \end{aligned}$$

For the given values, we have:

$$\begin{aligned} c_2^{-1} &\equiv 347 \pmod{3571}, \\ m_2 &\equiv 1393 \cdot 347 \cdot 567 \pmod{3571} \\ &\equiv 678 \pmod{3571}. \end{aligned}$$