

Cryptography

Assignment 5

Michael Orlov (orlovm@cs.bgu.ac.il)

Yanik Gleyzer (yanik@cs.bgu.ac.il)

June 9, 2003

Abstract

Solution for Assignment 5. One-way functions are assumed to be computable in polynomial time.

1 Question 1

In RSA signature scheme, public key is $\langle N, e \rangle$, and private key is $\langle N, d \rangle$, where $N = pq$ for big primes p, q , and $ed \equiv 1 \pmod{\varphi(N)}$.

We consider a modification of this scheme, where the signature on $M \in \mathbb{Z}_N^*$ is given by

$$\text{sig}(M) = (M + 1)^d \pmod{N}$$

1.1 Signature verification

Verifying signature is very similar to the original scheme:

$$\text{ver}(M, C) = [C^e \equiv M + 1 \pmod{N}]$$

Indeed, for $M, C \in \mathbb{Z}_N^*$,

$$\begin{aligned} \text{ver}(M, C) = \text{true} &\Leftrightarrow C^e \equiv M + 1 \pmod{N} \\ &\Leftrightarrow C^{ed} \equiv (M + 1)^d \pmod{N} \\ &\Leftrightarrow C \equiv (M + 1)^d \pmod{N} \quad \text{by Euler's Theorem} \\ &\Leftrightarrow C = \text{sig}(M) \end{aligned}$$

1.2 Chosen message attack

Given a message M , the attacker can choose random $M_1 \in \mathbb{Z}_N^*$, and compute $M_2 = (M + 1)M_1^{-1} \pmod{N}$. He then can ask the legal signer to sign on $M_1 - 1$ and $M_2 - 1$:

$$C_1 = \text{sig}(M_1 - 1)$$

$$C_2 = \text{sig}(M_2 - 1)$$

It is then straightforward to compute signature on M :

$$\begin{aligned}
 C_1 C_2 &\equiv \text{sig}(M_1 - 1) \text{sig}(M_2 - 1) && (\text{mod } N) \\
 &\equiv (M_1 - 1 + 1)^d (M_2 - 1 + 1)^d && (\text{mod } N) \\
 &\equiv M_1^d (M + 1)^d (M_1^{-1})^d && (\text{mod } N) \\
 &\equiv (M + 1)^d && (\text{mod } N) \\
 &\equiv \text{sig}(M) && (\text{mod } N)
 \end{aligned}$$

that is, $C_1 C_2 \text{ mod } N$ is a legal signature on M .

1.3 Single chosen message attack

It is possible to perform successful chosen message attack by asking for signature on only one message. Suppose that we want to obtain legal signature on message M .

If $M \equiv -1 \pmod{N}$, $\text{sig}(M) = 0$, and the signature is already known. Otherwise, we will ask for signature on $(-M - 2) \text{ mod } N$, where $(-M - 2) \not\equiv M \pmod{N}$, since the only solution to this equation is $M \equiv -1 \pmod{N}$ (assuming that $2 \in \mathbb{Z}_N^*$, which holds since N is odd).

Thus, we obtain

$$\begin{aligned}
 C' &= \text{sig}(-M - 2) \\
 &= (-M - 2 + 1)^d \pmod{N} \\
 &= (-1)^d (M + 1)^d \pmod{N} \\
 &= (-1)^d \text{sig}(M) \pmod{N} \\
 &= -\text{sig}(M) \pmod{N} \quad d \in \mathbb{Z}_{\varphi(N)}^* \text{ is odd, since } \varphi(N) \text{ is even}
 \end{aligned}$$

and

$$\text{sig}(M) = -C' \text{ mod } N$$

2 Question 2

In ElGamal signature system, the verification key is $\langle p, g, B \rangle$, with $B = g^b$ where $\langle p, g, b \rangle$ is the signature key.

2.1 Computing b using additional knowledge

Let m_1, m_2 be two messages with legal signatures $(\gamma_1, \delta_1), (\gamma_2, \delta_2)$. Suppose Eve succeeded in computing $a \in \mathbb{Z}_{p-1}$, such that $\gamma_1 \equiv g^a \gamma_2 \pmod{p}$. We now show how Eve can efficiently compute the signature key $\langle p, g, b \rangle$ using this information.

First, since $\text{ver}(m_1, (\gamma_1, \delta_1)) = \text{ver}(m_2, (\gamma_2, \delta_2)) = \text{true}$, we have

$$\begin{aligned}
 g^{m_1} &= B^{\gamma_1} \gamma_1^{\delta_1} && (\text{mod } p) \\
 g^{m_2} &= B^{\gamma_2} \gamma_2^{\delta_2} && (\text{mod } p)
 \end{aligned}$$

Substituting $\gamma_1 \equiv g^a \gamma_2 \pmod{p}$, and noting that since g is a primitive element modulo p , there exists $k_2 \in \mathbb{Z}_{p-1}$ such that $g^{k_2} \equiv \gamma_2 \pmod{p}$, and also substituting $B \equiv g^b \pmod{p}$,

$$\begin{aligned} g^{m_1} &= g^{b\gamma_1} (g^a g^{k_2})^{\delta_1} \pmod{p} \\ g^{m_2} &= g^{b\gamma_2} (g^{k_2})^{\delta_2} \pmod{p} \end{aligned}$$

Using Euler's Theorem, we get system of equations for powers of g :

$$\begin{aligned} m_1 &= b\gamma_1 + (a + k_2)\delta_1 \pmod{p-1} \\ m_2 &= b\gamma_2 + k_2\delta_2 \pmod{p-1} \end{aligned}$$

when we can eliminate k_2 by multiplying the first equation by δ_2 , and the second by δ_1 :

$$\begin{aligned} m_1\delta_2 &= b\gamma_1\delta_2 + (a + k_2)\delta_1\delta_2 \pmod{p-1} \\ m_2\delta_1 &= b\gamma_2\delta_1 + k_2\delta_2\delta_1 \pmod{p-1} \end{aligned}$$

and subtracting

$$m_1\delta_2 - m_2\delta_1 = b(\gamma_1\delta_2 - \gamma_2\delta_1) + a\delta_1\delta_2$$

Thus, assuming that $(\gamma_1\delta_2 - \gamma_2\delta_1)$ has inverse modulo $p-1$, Eve can efficiently calculate

$$b = (m_1\delta_2 - m_2\delta_1 - a\delta_1\delta_2)(\gamma_1\delta_2 - \gamma_2\delta_1)^{-1} \pmod{p-1}$$

which reveals the signature key $\langle p, g, b \rangle$.

2.2 Using same k

Under the simplistic assumption that $(\gamma_1\delta_2 - \gamma_2\delta_1)$ has inverse modulo $p-1$, Eve can recover the signature key if two messages have been signed using the same k :

$$\gamma_1 \equiv g^k \equiv \gamma_2 \pmod{p}$$

and since g is a primitive element modulo $p-1$, and $g^{p-1} \equiv 1 \pmod{p}$, we can substitute $a = p-1 \equiv 0 \pmod{p-1}$ in the result of Sec. 2.1:

$$\begin{aligned} b &= (m_1\delta_2 - m_2\delta_1 - a\delta_1\delta_2)(\gamma_1\delta_2 - \gamma_2\delta_1)^{-1} \pmod{p-1} \\ &= (m_1\delta_2 - m_2\delta_1)(\gamma_1\delta_2 - \gamma_2\delta_1)^{-1} \pmod{p-1} \end{aligned}$$

Assuming $\gamma_1 \equiv \gamma_2 \pmod{p-1}$ as well (which is probably true, since $\gamma_1 \equiv \gamma_2 \pmod{p}$), this can be simplified to

$$b = (m_1\delta_2 - m_2\delta_1)(\gamma_1(\delta_2 - \delta_1))^{-1} \pmod{p-1}$$

3 Question 3

Let p be prime, $p = 2w + 1$, where 2 and w are primitive elements modulo p .

3.1 Elements in \mathbb{Z}_p^*

Lemma 3.1. For all $x \in \mathbb{Z}_p^*$, it holds that $x^w \in \{1, -1\} \pmod{p}$.

Proof. Since p is prime, and $x \not\equiv 0 \pmod{p}$, it holds that

$$\left(\frac{x}{p}\right) \in \{1, -1\}$$

By Euler's Criterion,

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \equiv x^w \pmod{p}$$

□

Lemma 3.2.

$$w^{w-1} \equiv 2 \pmod{p} \tag{3.1}$$

Proof.

$$\begin{aligned} w^{w-1} &\equiv w^{\frac{p-1}{2}-1} \pmod{p} \\ &\equiv w^{\frac{p-1}{2}} w^{-1} \pmod{p} && w \in \mathbb{Z}_p^* \\ &\equiv -1 \cdot w^{-1} \pmod{p} && w \text{ is a primitive element modulo } p \\ &\equiv -\left(\frac{p-1}{2}\right)^{-1} \pmod{p} \\ &\equiv -(-1)^{-1}(2^{-1})^{-1} \pmod{p} \\ &\equiv 2 \pmod{p} \end{aligned}$$

□

3.2 Finding z

Suppose $\langle p, 2, B \rangle$ is the public key in an ElGamal signature system. If we define

$$z = \begin{cases} 0 & \text{if } B^w \equiv 1 \pmod{p} \\ 1 & \text{if } B^w \equiv -1 \pmod{p} \end{cases}$$

then z is well-defined by Lemma 3.1, and

$$\begin{aligned} 2^{wz} &\equiv \left(2^{\frac{p-1}{2}}\right)^z \pmod{p} \\ &\equiv (-1)^z \pmod{p} && 2 \text{ is a primitive element modulo } p \\ &\equiv B^w \pmod{p} && \text{by definition of } z \end{aligned}$$

Thus, by using the repetitive squaring algorithm, z can be computed efficiently.

3.3 Legal signature

For $m \in \mathbb{Z}_p^*$, defining $\delta = (w-1)(m-wz) \pmod{(p-1)}$ results in legal signature (w, δ) :

$$\begin{aligned} B^w w^\delta &\equiv B^w w^{(w-1)(m-wz)} \pmod{p} && \text{by Euler's Theorem} \\ &\equiv B^w 2^{m-wz} \pmod{p} && \text{by (3.1)} \\ &\equiv B^w 2^m (2^{wz})^{-1} \pmod{p} \\ &\equiv 2^m \pmod{p} && \text{by Sec. 3.2} \end{aligned}$$

4 Question 4

Let $f : \tau^n \rightarrow \tau^n$ be a one-way injective function. In this question, we consider function to be one-way if it is *preimage-resistant*. We note that since f is injective, and its domain and range are finite and equal, then f is also a bijection, and for each y there is exactly one x such that $y = f(x)$.

Lemma 4.1. Function $g_1 : \tau^n \rightarrow \tau^n$, given by

$$g_1(x) = f(f(x))$$

is a one-way function.

Proof. Assume by contradiction that g_1 is not a one-way function, that is, from given $y = g_1(x)$ it is possible to find x with some non-neglected probability p . Since f is injective, so is $f^2 = g_1$.

Then, given $y' = f(x)$, we can compute $y = f(y') = f(f(x)) = g_1(x)$, and retrieve (the unique) x with non-neglected probability p , which is a contradiction to f being a one-way function. Therefore, g_1 is also a one-way function. \square

Lemma 4.2. Function $g_2 : \tau^n \times \tau^n \rightarrow \tau^{2n}$, given by

$$g_2(x_1, x_2) = \langle f(x_1), f(x_2) \rangle$$

is a one-way function.

Proof. Assume by contradiction that g_2 is not a one-way function, that is, from given $\langle y_1, y_2 \rangle = g_2(x_1, x_2)$ it is possible to find x_1 and x_2 with some non-neglected probability p . By argument similar to the one in Lemma 4.1, g_2 is injective.

Then, given $y' = f(x)$, we can define $\langle y', y' \rangle = \langle f(x), f(x) \rangle = g_2(x, x)$, and retrieve (the unique) x with non-neglected probability p , which is a contradiction to f being a one-way function. Therefore, g_2 is also a one-way function. \square

Lemma 4.3. Function $g_3 : \tau^n \times \tau^n \rightarrow \tau^n$, given by

$$g_3(x_1, x_2) = f(x_1) \oplus x_2$$

is not a one-way function.

Proof. We will show that g_3 is not one-way by providing an efficient algorithm for finding some x_1 and x_2 such that

$$g_3(x_1, x_2) = y$$

for given y .

First, the algorithm picks $x_1 \in \tau^n$ and computes $f(x_1)$. Then, x_2 is computed to be $y \oplus f(x_1)$. Consequently,

$$g_3(x_1, x_2) = f(x_1) \oplus x_2 = f(x_1) \oplus y \oplus f(x_1) = y$$

and thus g_3 is not one-way. \square

5 Question 5

We consider a one-way injective function $f : \tau^n \rightarrow \tau^n$, and $m = 2n$.

5.1 g -function

The function $g : \tau^m \rightarrow \tau^m$ consists of 16 rounds,

$$\begin{aligned} x_{i+1} &= y_i \\ y_{i+1} &= x_i \oplus f(y_i) \end{aligned}$$

for $0 \leq i \leq 15$.

It is easy to see that $g(x_0, y_0) = \langle x_{16}, y_{16} \rangle$ is not a one-way function, since constructing g^{-1} is straightforward:

$$\begin{aligned} y_i &= x_{i+1} \\ x_i &= y_{i+1} \oplus f(y_i) \end{aligned}$$

and by applying 16 of such reverse rounds to $\langle x_{16}, y_{16} \rangle$, we will compute x_0 and y_0 in polynomial time.

5.2 h -function

The function $h : \tau^m \rightarrow \tau^m$ consists of two rounds,

$$\begin{aligned} x_{i+1} &= y_i \\ y_{i+1} &= y_i \oplus f(x_i) \end{aligned}$$

for $0 \leq i \leq 1$.

Lemma 5.1. h is a one-way function.

Proof. Let us compute $h(x, y)$:

$$\begin{aligned} h(x, y) &= \langle x_2, y_2 \rangle \\ &= \langle y_1, y_1 \oplus f(x_1) \rangle \\ &= \langle y_0 \oplus f(x_0), y_0 \oplus f(x_0) \oplus f(y_0) \rangle \\ &= \langle y \oplus f(x), y \oplus f(x) \oplus f(y) \rangle \end{aligned}$$

Assume by contradiction that h is not a one-way function. Then, for given $\langle x', y' \rangle$, it is possible to find x, y (with some non-neglected probability p , and in polynomial time) such that

$$\langle x', y' \rangle = h(x, y) = \langle y \oplus f(x), y \oplus f(x) \oplus f(y) \rangle$$

We then note that

$$h(x, 0^n) = \langle f(x), f(x) \oplus f(0^n) \rangle$$

and by finding $h^{-1}(\langle f(x), f(x) \oplus f(0^n) \rangle)$, we will compute (the unique, since f is injective over finite domain, which is the same as its range, and is thus a bijection) x with non-neglected probability p , which is a contradiction to f being a one-way function. Therefore, h is a one-way function as well. \square

References

- [1] Douglas R. Stinson. *Cryptography: Theory and Practice*. Discrete Mathematics and its Applications. CRC Press, second edition, 2002.