HIT — Cryptography — Solutions 5

1603202-1150810613-Qiuhao Li

December 31, 2018

Problem 1. Compute $[101^{4,800,000,023} \bmod 35]$ (by hand).

Solution 1.

$$\because \phi(35) = (7-1) * (5-1) = 24$$
$$\therefore [[101 \bmod 35]^{[4,800,000,023 \bmod \phi(35)]} \bmod 35] = [31^{-1} \bmod 35]$$

Extended Euclidean algorithm:

$$31x + 35y \equiv 1 \bmod 35$$
$$\Rightarrow x \equiv 26 \equiv 31^{-1} \bmod 35$$

So we conclude:

$$101^{4,800,000,023} \equiv 26 \bmod 35$$

Problem 2. Let $N = pq$ be a product of two distinct primes. Show that if $\phi(N)$ and N are known, then it is possible to compute p and q in polynomial time.

Solution 2.

Proof.

Let's say c_x means constant. We know $\phi(N) = (p-1) * (q-1) = c_1$ and $N = p * q = c_2$, which indicate that $c_2 - p - q + 1 = c_1$ and $p = c_3 - q$. So $(c_3 - q) * q = c_2$, thus compute p and q in polynomial time.

□

Problem 3. For an RSA public key $\langle N, e \rangle$, we have an algorithm $\mathcal{A}$ that always correctly computes $LSB(x)$ given $[x^e \mod N]$. Design an algorithm that computes x from $[x^e \mod N]$.

Solution 3.

Input: $c = x^e \mod N$, $\langle N, e \rangle$
Output: $x \mod N$

```
result = [];
for j = 0; j < lengthof(x); j = j + 1 do
    c' = (2^{-j})^e · c
    bit b = Give c' to A, computes LSB(c')
    result = b||result
end
return result;
```

Algorithm 1: Computes x from $[x^e \mod N]$

Problem 4. Consider the following key-exchange protocol:

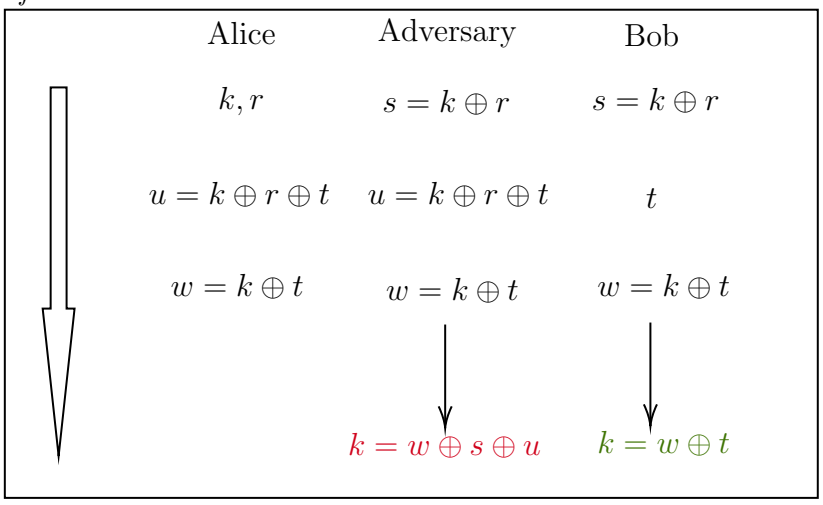
1. Alice chooses $k, r \leftarrow \{0,1\}^n$ at random, and sends $s := k \oplus r$ to Bob.
2. Bob chooses $t \leftarrow \{0,1\}^n$ at random and sends $u := s \oplus t$ to Alice.
3. Alice computes $w := u \oplus r$ and sends w to Bob.
4. Alice outputs k and Bob computes $w \oplus t$.

Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e. either prove its security or show a concrete attack by an eavesdropper).

Solution 4.

This key-exchange protocol do make sure the Alice and Bob output the same key, but the adversary can also generate the key.

Proof.



□

Problem 5. Consider the following public-key encryption scheme. The public key is $(\mathbb{G}, q, g, h)$ and the private key is x, generated exactly as in the El Gamal encryption scheme. In order to encrypt a bit b, the sender does the following:

- If $b = 0$ then choose a random $y \leftarrow \mathbb{Z}_q$ and compute $c_1 = g^y$ and $c_2 = h^y$. The ciphertext is $\langle c_1, c_2 \rangle$.
- If $b = 1$ then choose independent random $y, z \leftarrow \mathbb{Z}_q$ and compute $c_1 = g^y$ and $c_2 = g^z$, and set the ciphertext is $\langle c_1, c_2 \rangle$.

(a) Show that it is possible to decrypt efficiently given knowledge of x. (b) Prove that this encryption scheme is CPA-secure if the decisional Diffie-Hellman problem is hard relative to $\mathcal{G}$

Solution 5.

Most of this answer refers to Mr. Zhang Yu's slides.

- if $c_2/c_1^x = 1$ then $Dec := 0$, else $Dec := 1$ with possibility of $(q-1)/q$

  Proof.

  If $b = 0$, then $c_2 = h^y = g^{xy}$, and $c_1^x = g^{xy}$, thus making $c_2/c_1^x = 1$.

  Else if $b = 1$, then $c_2/c_1^x = g^z/g^{xy}$, but y and z are independent random number. So for any random number $k \leftarrow \mathbb{Z}_q$, include 1, the possibility of $c_2/c_1^x = k$ equals $1/q$. □

- *Proof.*

  Idea: Prove that Π is secure in the presence of an eavesdropper by reducing an algorithm D for DDH problem to the eavesdropper $\mathcal{A}$.

  Modify Π to $\tilde{\Pi}$: the encryption is done by choosing random $y \leftarrow \mathbb{Z}_q$ and $z \leftarrow \mathbb{Z}_q$ and outputting the ciphertext:

  $$\langle g^y, g^z \cdot m \rangle.$$

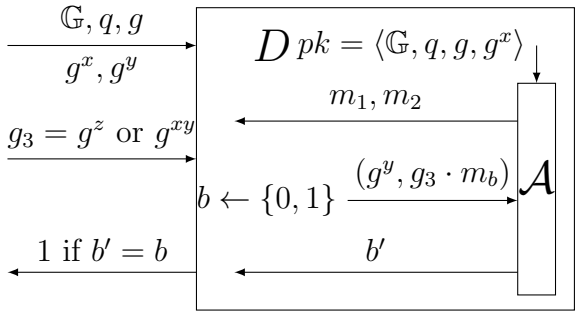
  - $\tilde{\Pi}$ is not an encryption scheme.
  - g^y is independent of m.
  - $g^z \cdot m$ is a random element independent of m, which means:

  $$\Pr\left[\mathsf{PubK}^{\mathsf{eav}}_{\mathcal{A},\tilde{\Pi}}(n) = 1\right] = \frac{1}{2}.$$

  D receives $(\mathbb{G}, q, g, g^x, g^y, g_3)$ where g_3 equals either g^{xy} or g^z, for random x, y, z:

  Case I: $g_3 = g^z$, ciphertext is $\langle g^y, g^z \cdot m_b \rangle$.
  As mentioned above, when $b = 1$, the 'fake' g^{xy} we calculated using Dec has no difference with a random number g^z, so this case matches the situation of $b = 1$.

  $$\Pr[D(g^x, g^y, g^z) = 1] = \Pr\left[\mathsf{PubK}^{\mathsf{eav}}_{\mathcal{A},\tilde{\Pi}}(n) = 1\right] = \frac{1}{2}.$$



Case II: $g_3 = g^{xy}$, ciphertext is $\langle g^y, g^{xy} \cdot m_b \rangle$.
And this case matches the situation of $b = 0$.

$$\Pr[D(g^x, g^y, g^{xy}) = 1] = \Pr\left[\mathsf{PubK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1\right] = \varepsilon(n).$$

Since the DDH problem is hard,

$$\mathsf{negl}(n) \geq |\Pr[D(g^x, g^y, g^z) = 1] - \Pr[D(g^x, g^y, g^{xy}) = 1]| = |\frac{1}{2} - \varepsilon(n)|.$$

So no matter $b = 0$ or $b = 1$, any $polynomial - time$ adversary can never figure out the plaintext with possibility better than $\frac{1}{2} + \mathsf{negl}(n)$. □

Problem 6. The natural way of applying hybrid encryption to the El Gamal encryption scheme is as follows. The public key is $pk = \langle \mathbb{G}, q, g, h \rangle$ as in the El Gamal scheme, and to encrypt a message m the sender chooses random $k \leftarrow \{0,1\}^n$ and sends

$$\langle g^r, h^r \cdot k, \mathsf{Enc}_k(m) \rangle,$$

where $r \leftarrow \mathbb{Z}_q$ is chosen at random and Enc represents a private-key encryption scheme. Suggest an improvement that results in a shorter ciphertext containing only a *single* group element followed by a private-key encryption of m.

Solution 6.

Improvement: Let $k = h^r = g^{xr}$, in which r is chosen at random, and send

$$\langle g^r, \mathsf{Enc}_{h^r}(m) \rangle$$

Problem 7. For each of the following variants of the definition of security for signatures, state whether textbook RSA is secure and prove your answer:

- (a) In this first variant, the experiment is as follows: the adversary is given the public key pk and a random message m. The adversary is then allowed to query the signing oracle once on a single message that does not equal m. Following this, the adversary outputs a signature σ and succeeds if $\mathsf{Vrfy}_{pk}(m, \sigma) = 1$. As usual, security is said to hold if the adversary can succeed in this experiment with at most negligible probability.

- (b) The second variant is as above, except that the adversary is not allowed to query the signing oracle at all.

Solution 7.

- It's not secure. To forge a signature on m, we can choose a random m_1, set $m_2 := [m/m_1 \bmod N]$, obtain signatures σ_1, σ_2 on m_1, m_2. Then $\sigma := [\sigma_1 * \sigma_2 \bmod N]$ is a valid signature on m.
- It's secure. Simply put, to calculate d which meets $[e = d^{-1} \bmod N]$ given only $[m^e \bmod N]$, either the adversary solves large-prime factorization problem or discrete logarithm problem — both are very difficult problem in number theory.

Problem 8. Consider the Lamport one-time signature scheme. Describe an adversary who obtains signatures on two messages of its choice and can then forge signatures on any message it likes.

Solution 8.

The adversary signatures on $m_1 = 0^\ell$ and $m_2 = 1^\ell$, by which he can get $\sigma = (x_{1,0}, \ldots, x_{\ell,0})$ and $\sigma = (x_{1,1}, \ldots, x_{\ell,1})$, thus obtaining the

$$sk = \begin{pmatrix} x_{1,0} & x_{2,0} & \cdots & x_{\ell,0} \\ x_{1,1} & x_{2,1} & \cdots & x_{\ell,1} \end{pmatrix}.$$

Happy  Hacking!