Notes on Problem Set 5

2. Let p and q be primes such that $p = 2q + 1$. Let α be a random element of Z_p^*. Prove that if neither $\alpha^2 \bmod p$ nor $\alpha^q \bmod p$ is equal to 1, then α is a generator of Z_p^*.

Proof We have

$$\begin{aligned} \phi(p) &= p - 1 \quad \text{(since } p \text{ is prime)} \\ &= 2q \quad \text{(since } p = 2q + 1\text{)} \end{aligned}$$

We know that $order(\alpha)$ (the order of α) divides $\phi(p)$. Therefore, $order(\alpha)$ divides $2q$. But since q is prime, the only nontrivial divisors of $2q$ are 2, q, and $2q$. Hence the only possible values of $order(\alpha)$ are 2, q, or $2q$. Since neither $\alpha^2 \bmod p$ nor $\alpha^q \bmod p$ is equal to 1, $order(\alpha)$ can't be 2 or q. Therefore, $order(\alpha) = 2q = \phi(p)$. By definition, this means that α is a generator of Z_p^*.

3. Stinson, problem 5.12(a), p.181.

Recall that if x_1 and x_2 have length $2m$, and $x = x_1||x_2$, then

$$h_2(x) = h_1(h_1(x_1)||h_1(x_2)).$$

We want to show that if h_1 is collision resistant, then so is h_2. We'll proceed by proving the (logically equivalent) contrapositive: if h_2 is *not* collision resistant, then neither is h_1.

So assume that we have found a collision for h_2. That is, we have found $x \neq x'$, where x and x' both have length $4m$, such that $h_2(x) = h_2(x')$. We want to show that, in this case, we can easily find a collision for h_1.

In keeping with Stinson's notation, we can express x and x' as follows:

$$\begin{aligned} x &= x_1 \parallel x_2 \\ x' &= x_1' \parallel x_2' \end{aligned}$$

[**Notes**

i. Some of you argued that since

$$h_2(x) = h_1(h_1(x_1) \parallel h_1(x_2)) = h_1(h_1(x_1') \parallel h_1(x_2')) = h_2(x'),$$

it must follow that

$$h_1(x_1) \parallel h_1(x_2) = h_1(x_1') \parallel h_1(x_2').$$

But this doesn't follow at all. Remember that hash functions are many-one. There are many inputs that produce a given output. Thus, from the fact that $h(a) = h(b)$, it definitely does not follow that $a = b$.

ii. On the other hand, some of you argued like this:

We're given that $x_1 \parallel x_2 \neq x'_1 \parallel x'_2$.

Therefore, $h_1(x_1) \parallel h_1(x_2) \neq h_1(x'_1) \parallel h_1(x'_2)$.

Since

$$h_1(h_1(x_1) \parallel h_1(x_2)) = h_2(x) = h_2(x') = h_1(h_1(x'_1) \parallel h_1(x'_2)),$$

we immediately have a collision for h_1.

The problem with this argument is that

$$h_1(x_1) \parallel h_1(x_2) \neq h_1(x'_1) \parallel h_1(x'_2)$$

does not follow from

$$x_1 \parallel x_2 \neq x'_1 \parallel x'_2.$$

Why should it? It may well be true that $h_1(x_1) \parallel h_1(x_2) \neq h_1(x'_1) \parallel h_1(x'_2)$; on the other hand, it may be that $h_1(x_1) \parallel h_1(x_2) = h_1(x'_1) \parallel h_1(x'_2)$. So we have to proceed by cases.]

Case 1 Suppose that $h_1(x_1) \neq h_1(x'_1)$. then

$$h_1(x_1) \parallel h_1(x_2) \neq h_1(x'_1) \parallel h_1(x'_2).$$

But we're assuming that $h_2(x) = h_2(x')$. By the definition of h_2, this means that

$$h_1(h_1(x_1) \parallel h_1(x_2)) = h_1(h_1(x'_1) \parallel h_1(x'_2)),$$

and so we have found a collision for h_1.

Case 2 $h_1(x_2) \neq h_1(x'_2)$. Apply the same argument used in Case 1.

Case 3 $h_1(x_1) = h_1(x'_1)$ and $h_1(x_2) = h_1(x'_2)$. Since we're assuming that $x \neq x'$, we must have

$$x_1 \parallel x_2 \neq x'_1 \parallel x'_2.$$

Therefore, either $x_1 \neq x'_1$ or $x_2 \neq x'_2$. In either case, we have a collision for h_1.

Since these cases are exhaustive, it follows that we can always find a collision for h_1, given a collision for h_2. Therefore, collision resistance for h_1 implies collision resistance for h_2.

4.

i. Suppose Bob uses ElGamal to encrypt two different messages to Alice, but carelessly uses the same random k (same ephemeral key) for both encryptions. Thus Bob creates the ciphertexts,

1. (γ, δ_1)
2. (γ, δ_2)

Suppose that you have intercepted both ciphertexts; know Alice's public parameter p; *and* have discovered the plaintext m_1 corresponding to the first ciphertext. Describe an algorithm for finding the second plaintext m_2.

Solution By definition of ElGamal encryption,

$$(\gamma, \delta_1) \equiv (g^k, m_1 g^{ak}) \bmod p \tag{1}$$

$$(\gamma, \delta_2) \equiv (g^k, m_2 g^{ak}) \bmod p \tag{2}$$

From (1), we have

$$\delta_1 \equiv m_1 g^{ak} \bmod p.$$

Therefore,

$$g^{ak} \equiv m_1^{-1} \delta_1 \bmod p.$$

Since we know both m_1 and δ_1, this last equation gives us $g^{ak} \bmod p$. Therefore, we can compute m_2 from equation (2):

$$m_2 \equiv g^{-ak} \delta_2 \bmod p.$$

ii. Apply the method described in part (i) to find the plaintext corresponding to the second ciphertext in the following example. The two ciphertexts are

1. (1430, 697)
2. (1430, 1113).

You have intercepted the ciphertexts, know Alice's public parameter $p = 2357$, and have discovered that the plaintext corresponding to the first ciphertext (1430,697) is 2035.

Solution By definition of ElGamal encryption,

$$(g^k, m_1 g^{ak}) \equiv (1430, 697) \bmod 2357.$$

In particular,

$$m_1 g^{ak} \equiv 697 \bmod 2357.$$

We're given that $m_1 = 2035$. Therefore,

$$g^{ak} \equiv 2035^{-1} \cdot 697 \equiv 2174 \cdot 697 \equiv 2084 \bmod 2357.$$

Looking at the second ciphertext, we know (again by definition of ElGamal encryption) that

$$m_2 \cdot g^{ak} \equiv 1113 \bmod 2357.$$

Therefore,

$$m_2 \equiv (g^{ak})^{-1} \cdot 1113 \equiv 2084^{-1} \cdot 1113 \equiv 872 \cdot 1113 \equiv 1809 \bmod 2357.$$

So 1809 is the second plaintext.

5. Suppose that the ElGamal Signature Scheme is applied to two different messages x_1 and x_2, using the *same* value of k. Thus we obtain two signatures (r, s_1), (r, s_2). Assume further that $gcd(s_1 - s_2, p - 1) = 1$, and that the messages x_1 and x_2 are known. Then we can easily calculate k in the following way.

By definition,

$$\begin{aligned} s_1 &= k^{-1}(h(x_1) - ar) \bmod (p-1) && (3) \\ s_2 &= k^{-1}(h(x_2) - ar) \bmod (p-1) && (4) \end{aligned}$$

Applying our basic facts on modular equivalence to equations (1) and (2),

$$\begin{aligned} ks_1 &\equiv (h(x_1) - ar) \bmod (p-1) && (5) \\ ks_2 &\equiv (h(x_2) - ar) \bmod (p-1) && (6) \end{aligned}$$

Subtracting (4) from (3),

$$k(s_1 - s_2) \equiv (h(x_1) - h(x_2)) \bmod (p-1). \quad (7)$$

Now the fact that $gcd(s_1 - s_2, p - 1) = 1$ ensures that $(s_1 - s_2)$ has an inverse $\bmod (p-1)$. Therefore, applying our basic facts to (5), we obtain

$$k \equiv (s_1 - s_2)^{-1}(h(x_1) - h(x_2)) \bmod (p-1).$$

We know all of the terms on the right-hand side of the equivalence, and hence can easily compute k.