CS 435 Final
Zhaoyi Zhang
zzhang825

1. Assume the elements of S is uniformly selected from G.
To compute the discrete log of arbitrary element g^x of G, where $x \in \mathbb{Z}_q$, generate a random number $r \in \mathbb{Z}_q$ uniformly, and compute $g^x \cdot g^r$ and divide it by g^{q-1} if it's greater than g^{q-1}.
In other words, $g^{(x+r) \bmod q}$ is computed.
Since r is generated uniformly, r and $(x+r) \bmod q$ has a $\frac{k}{q}$ probability such that $g^{(x+r) \bmod q} \in S$. If so, Eve can compute the discrete log of $g^{(x+r) \bmod q}$, obtain $(x+r) \bmod q$ and finally obtain $x = ((x+r) \bmod q) - r) \bmod q$
Therefore, Eve can compute the discrete log of arbitrary element of G with probability $\frac{k}{q}$

2. If $x \equiv yz \pmod n$, we know $z = y^{-1} \cdot x \bmod n$, because

$x \equiv y \cdot y^{-1} \cdot x \pmod n$

$x \equiv 1 \cdot x \pmod n$

$x \equiv x \pmod n$

Thus, such z exists if and only if y has a multiplicative inverse

Statement 1 is false, because for some $x, y \in \mathbb{Z}_n$, $\gcd(x,n) \neq 1$ or $\gcd(y,n) \neq 1$ y will not have a multiplicative inverse

Statement 2 is true, because for all $x, y \in \mathbb{Z}_n^*$, $\gcd(x,n) = \gcd(y,n) = 1$, y must have a multiplicative inverse $y^{-1} \in \mathbb{Z}_n^*$ which can be computed by Extended Euclidean Algorithm.

A counter example of statement 1 could be $\mathbb{Z}_6$

Let $x = 1$ and $y = 4$.

There does not exist a $z \in \mathbb{Z}_6$ such that $1 \equiv 4z \pmod 6$

3. (i) Let GenRSA be a PPT algorithm that, on input 1^n, outputs N which is a product of two n-bit primes, along with e, d such that $ed \equiv 1 \pmod{\phi(N)}$

Define a RSA signature schemes as follows:

Gen: on input 1^n, run GenRSA(1^n) to obtain (N, e, d).
The public key is $\langle N, e \rangle$ and the private key is $\langle N, d \rangle$

Sign: on input a private key $sk = \langle N, d \rangle$ and a message $m \in \mathbb{Z}_N^*$ compute the signature $\sigma := [m^d \bmod N]$

Vrfy: on input a public key $pk = \langle N, e \rangle$, a message $m \in \mathbb{Z}_N^*$ a signature $\sigma \in \mathbb{Z}_N^*$, output 1 iff $m \stackrel{?}{=} [\sigma^e \bmod N]$

3(ii) Solve $\sigma \equiv m^d \bmod N$ where $N = pq$. p, q are primes.
Assume exponentiation modulo an l-bit integer takes $r \cdot l^3$ operations where r is a constant. If p, q are each n bits, then computing $m^d \bmod N$ takes $r(2n)^3 = 8r \cdot n^3$ operations, because $|N| = 2n$

Using CRT, we can solve the following system of equations instead

$$\begin{cases} \sigma \equiv m^d \pmod p \\ \sigma \equiv m^d \pmod q \end{cases}$$

Let $d = (p-1)L + r$ where $r = d \bmod (p-1)$

$m^d \equiv m^{(p-1)L} \cdot m^r \pmod p$

By FLT, $m^{p-1} \equiv 1 \bmod p$.

Thus $m^{(p-1)L} \cdot m^r \bmod p = 1^L \cdot m^r \bmod p = m^r \bmod p$.

Use the same argument for q, we get:

$$\begin{cases} \sigma \equiv m^{d \bmod (p-1)} \pmod p \\ \sigma \equiv m^{d \bmod (q-1)} \pmod q \end{cases}$$

Let $a_p = m^{d \bmod (p-1)} \bmod p$, $a_q = m^{d \bmod (q-1)} \bmod q$

To comput a_p, a_q, we only need $r \cdot n^3$ operations each.

$$\begin{cases} \sigma \equiv a_p \pmod p \\ \sigma \equiv a_q \pmod q \end{cases}$$

By FLT. $q^{p-1} \equiv 1 \bmod p$ and $p^{q-1} \equiv 1 \bmod q$

Thus, $M_1 = q$ $\quad M_2 = p$

$N_1 = q^{p-2}$ $\quad N_2 = p^{q-2}$

The solution is $\sigma \equiv a_p \cdot q \cdot q^{p-2} + a_q \cdot p \cdot p^{q-2} \pmod N$

The time complexity of the signing step is reduced from $8r \cdot n^3$ to $2r \cdot n^3$

3(iii) no-message attack:

Given a public key $\langle N, e \rangle$, choose a uniform $\sigma \in \mathbb{Z}_N^*$ and compute $m := [\sigma^e \bmod N]$ and output (m, σ). By definition, it is a valid forgery.

multiplicative attack:

Given a message $m \in \mathbb{Z}_N^*$ and a public key $\langle N, e \rangle$, choose any messages $m_1, m_2 \in \mathbb{Z}_N^*$ such that $m = m_1 \cdot m_2 \bmod N$. Query the oracle with m_1, m_2 to get σ_1, σ_2. Compute $\sigma := [\sigma_1 \cdot \sigma_2 \bmod N]$ and output (m, σ)

It is a valid forgery, because

$\sigma^e = (\sigma_1 \cdot \sigma_2)^e = (m_1^d \cdot m_2^d)^e = m_1^{de} \cdot m_2^{de} = m_1 \cdot m_2 = m \bmod N$.

3(iv) In no-message attack, let $\hat{m} := [\sigma^e \bmod N]$. Then, a valid message m should satify $H(m) = \hat{m}$, which is hard according to pre-image resistent.

In multiplicative attack, a valid forgery m should satisfy $H(m) = H(m_1)H(m_2)$ for some m_1, m_2. This happens with negligible probability

4. Alice picks $x \leftarrow \mathbb{Z}_q$ and sends g^x to Bob
The man gets g^x from Alice, picks $x' \leftarrow \mathbb{Z}_q$ and sends $g^{x'}$ to Bob
Bob picks $y \leftarrow \mathbb{Z}_q$ and sends g^y to Alice
The man gets g^y from Bob, picks $y' \leftarrow \mathbb{Z}_q$ and sends $g^{y'}$ to Alice
Alice thinks the key is $k_A = (g^{y'})^x$ and Bob thinks the key is $k_B = (g^{x'})^y$

The man-in-the-middle attack can be prevented by using authenticated Diffe-Hellman key exchange.
Alice and Bob will send g^x and g^y along with digital signatures σ_A and σ_B, where $\sigma_A = Sign_{sk_A}(g^x)$, $\sigma_B = Sign_{sk_B}(g^y)$

Since the man-in-the-middle does not know sk_A and sk_B, it cannot compute σ_A and σ_B, and thus cannot impersonate Alice and Bob.

5. To forge a signature for $m \in \mathbb{Z}_N^*$, the adversary A sets
$m' = [m^{-1} \bmod N]$
A queries the oracle with m' and gets $\sigma' \leftarrow Sign_{sk}(m')$
where $Sign_{sk}(m') = [(m')^d \bmod N]$
A computes $\sigma = [(\sigma')^{-1} \bmod N]$ and outputs (m, σ)
(m, σ) is a valid forgery because

$$\sigma^e = (\sigma')^{-e} = (m')^{-ed} = m^{ed} = [m \bmod N]$$

6. $2x5 \equiv 1 \pmod 9$, so multiply $2x \equiv 2 \pmod 9$ with 5 on both sides to get $10x \equiv 10 \pmod 9$
Simplify it, we get $x \equiv 1 \pmod 9$

Similarly, multiply $4x \equiv 3 \pmod 5$ with 4, $5x \equiv 2 \pmod 7$ with 3
we get $x \equiv 2 \pmod 5$, $x \equiv 6 \pmod 7$

$$\begin{cases} x \equiv 1 \pmod 9 \\ x \equiv 2 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases}$$

$M_1 = 35$ $M_2 = 63$ $M_3 = 45$

$N_1 = 8$ $N_2 = 2$ $N_3 = 5$

$1 \times 35 \times 8 + 2 \times 63 \times 2 + 6 \times 45 \times 5 = 1882$

$1882 \bmod 315 = 307$

The solution is $x \equiv 307 \pmod{315}$