Nanjing University
Introduction to Cryptography
Fall 2023

Solution of Final 23

1. Hash function.

   (1) Not collision resistant. For a fixed Δ and given a hash h of message x, we can find a collision where $x' = x \oplus \Delta$ and $H_1(x') = h$.

   (2) Collision resistant. Assume there's an adversary A which can find a collision (x_1, x_2) for H_1, then (x_1, x_2) is also a collision for H.

2. Euler theorem.

   According to Euler theorem, we have $\alpha^{p-1} \equiv 1 \bmod p$, which means $\alpha^{\lambda(p-1)+1} \equiv \alpha \bmod p$. Because p is a prime with $p \equiv 2 \bmod 3$, $2p \equiv 1 \bmod 3$ such that $(2p-1)/3$ is a positive integer. Then we output $\sigma := \alpha^{(2p-1)/3}$ as a cube root of α.

3. Chinese remainder theorem.

   Assume that there are at least X people in the school, then we get the followings:

$$X \equiv 6 \bmod 9$$
$$X \equiv 2 \bmod 7$$
$$X \equiv 3 \bmod 5$$

   The numbers 5, 7, and 9 are pairwise coprime. The least common multiples of each pair are 35, 45, and 63. The least common multiple of all three numbers is 315.

   Next, we find the corresponding numbers 8, 5, and 2. We calculate 35*8=280, 45*5=225, 63*2=126.

   Finally, we calculate (280*6 + 225*2 + 126*3) mod 315 = 303.

4. RSA encryption.

   We know that $d \equiv e^{-1}$ (mod $\phi(N) = (p-1)(q-1)$). For this to happen, we need $\gcd(e, (p-1)(q-1))$ to be equal to 1. If we let $e = 2$, then we need for $\gcd(2, (p-1)(q-1)) = 1$, which means $(p-1)(q-1)$ must be odd. For this to happen, both $p-1$ and $q-1$ must be odd, making p, q both even. We know importantly, however, that the RSA method requires p and q to be primes, and the only even prime is 2. As we have determined what p and q must be, we can now solve for d, breaking the RSA system.

5. ElGamal encryption.

   (1) $c_B = \langle g^y \cdot g^f, h^f \cdot (h^y \cdot g^a) \rangle$, which equals $\langle g^{y+f}, h^{y+f} \cdot g^a \rangle$, is the encryption of g^a.

(2) $c_B = \langle (g^y)^{q-1} \cdot g^f, h^f \cdot g \cdot (g^a \cdot h^y)^{q-1} \rangle$, which is a valid encryption of $g^{a\cdot(q-1)+1}$. Since g has order q, c_B is thus the encryption of g^1 if $a = 0$, and g^0 if $a = 1$.

6. Signature scheme.

(1) Secure. Assume the scheme is not secure, i.e. there's an adversary A which can forge a signature (σ_0, σ_1) for a message m that can pass the verifier V_1 with non-negligible probability $\delta(n)$, then we can construct an adversary A' from A break the signature scheme (G, S, V). Assume there's a challenger C with key (sk'_0, pk'_0), A' runs G and get (sk'_1, pk'_1). When A query for a message m', A' query C for m' and get the signature σ'_0. A' also compute $\sigma'_1 = S(sk'_1, m)$ locally. A' then send (σ'_0, σ'_1) to A. When A return a forged signature $(m'', (\sigma''_0, \sigma''_1))$, A' return (m'', σ''_0). A' wins the game with probability $\Pr[A'wins] = \frac{1}{2}\delta(n)$, which is also a non-negligible probability.

(2) Not secure. Query $m_1 = (m_L^1, m_R^1)$ and get (σ_0^1, σ_1^1), query $m_2 = (m_L^2, m_R^2)$ and get (σ_0^2, σ_1^2). Then output a valid signature and its corresponding message $(m_3 = (m_L^1, m_R^2), (\sigma_0^1, \sigma_1^2)$.

~~(3) Not secure. Query m_1 and get (r, σ_0, σ_1), output $(r, (m, \sigma_0, \sigma_1))$.~~

Not secure. Query m1 and get (r1, σ 10, σ 11), query m2 and get (r2, σ 20, σ 21), output (m1⊕r2⊕r1, (r2, σ 10, σ 21))