0816028 周函諺

1. $RSAH(C1, C2) = RSA(RSA(C1) \oplus C2)$
$= RSA(RSA(C1) \oplus RSA(C1) \oplus RSA(B1) \oplus B2)$
$= RSA(RSA(B1) \oplus B2)$
$= RSA(B1, B2)$
$\Rightarrow C2 = RSA(C1) \oplus RSA(B1) \oplus B2$ ※

2. A user who produces a signature with $s=0$ is inadvertently revealing his or her private key d via the relationship:
$s = 0 = k^{-1}[H(m) + dr] \bmod q$
$d = \frac{-H(m)}{r} \bmod q$

3. $H(M) = 1111 = 15 = m$
(a) RSA
$n = 323 = 17 \times 19$
private key(d) = $(7^{-1} \bmod 288 = 247, 323)$

(a) RSA
$n = 323 = 17 \times 19$
private key(d) = $(7^{-1} \bmod 288 = 247, 323)$
public key(e) = 7
sign: PRA = $(247, 323)$
$m = 15$, $S = m^d \bmod n = 15^{247} \bmod 323 = 314$
$(M, S) = (\text{"Hello!"}, 314)$
verify: $m = 15$
$m = 15$
$m' = 314^n \bmod 323 = 15$
$\Rightarrow m = m'$ ※

(b) Elgamal
$q = 103$, $\alpha = 11$, private key $X_A = 35$, public key $Y_A = \alpha^{X_A} \bmod q = 11^{35} \bmod 103 = 101$
sign: random choose $k = 5$, $\gcd(5, 102) = 1$
$S_1 = \alpha^k \bmod q = 11^5 \bmod 103 = 62$
$S_2 = k^{-1}(m - X_A S_1) \bmod q - 1 = 41(15 - 35 \cdot 62) \bmod 102 = 79$
$(M, S_1, S_2) = (\text{"Hello!"}, 62, 79)$
varify: $m = 15$, $\alpha^m \bmod q = 11^{15} \bmod 103 = 89$
$Y_A^{S_1} S_1^{S_2} \bmod q = 101^{62} \cdot 62^{79} \bmod 103 = 89$
$\Rightarrow \alpha^m = Y_A^{S_1} S_1^{S_2} \bmod q$ ※

(c) Schnorr

$p=103, q=17, a=72$, private key $=(103, 17, 72, 10)$

$s=10$

$V = a^{-s} \bmod p = 72^{-10} \bmod 103 = 66$

sign: random choose $r=2$

$x = a^r \bmod p = 72^2 \bmod 103 = 34$

$e = H(M \| x) = 6$

$y = (r+se) \bmod q = (2+10 \cdot 6) \bmod 17 = 11$

$(e, y) = (6, 11)$

Varify: $x' = a^y v^e \bmod p = 72^{11} 66^6 \bmod 103 = 34$

$\Rightarrow e = H(M \| 34)$ ※

(d) DSA

$p=103, q=17, g=72$, private key $=(103, 17, 72, 7)$

$x=7$, $y = g^x \bmod p = 72^9 \bmod 103 = 66$

sign: $H(M)=15, k=3$

$r = g^k \bmod p \bmod q = 72^3 \bmod 103 \bmod 17 = 11$

$s = k^{-1}(H(M) + rx) \bmod q = 3^{-1}(15 + 11 \cdot 7) \bmod 17 = 8$

$(r, s) = (11, 8)$

Varify: $w = s^{-1} \bmod q = 8^{-1} \bmod 17 = 15$

$u_1 = H(M) \cdot w \bmod q = 15 \cdot 15 \bmod 17 = 4$

$u_2 = r \cdot w \bmod q = 11 \cdot 15 \bmod 17 = 12$

$v = g^{u_1} \cdot y^{u_2} \bmod p \bmod q = 72^4 \cdot 66^{12} \bmod 103 \bmod 17 = 11$

$\Rightarrow v = r$ ※