HW 2

1. (a) sign

$$S = M^d \bmod 33$$
$$= 25^7 \bmod 33 = 31$$

(b) verify

$$M' = S^e \bmod 33$$
$$= 31^3 \bmod 33$$
$$= 25 = M$$

2. $p=23,\ d=9,\ g=5,\ X=10$

Select $K_E = 7 \in Z_{22}$ s.t. $\gcd(7, 22)$

$K_E^{-1} = 19 \bmod 22$

sign

$$r = 5^7 \bmod 23$$
$$= \boxed{17} \bmod 23$$

$$S = (10 - 9 \cdot 17)\ 17^{-1} \bmod 22$$
$$= \boxed{11} \bmod 22$$

Alice $\xrightarrow{(10, (17, 22))}$ Bob

verify

$$V = \beta^r r^S \bmod p$$
$$= 11^9 \cdot 17^{11} \bmod 23$$
$$= 5^{10} \bmod 23$$

$(\beta = g^d \bmod p = 5^9 \bmod 23 = 11 \bmod 23)$

$$V' = g^X \bmod p$$
$$= 5^{10} \bmod 23 \quad \therefore V = V'$$

3. $p=27$, $q=13$. $X=5$, $H(x)=5$

choose $g=6$ s.t $g^q \equiv 1 \bmod p$

$(\gcd(g, p) = 1)$

Choose $d = 7$

(a) select $k=2$, $k^{-1} \bmod q = 2^{-1} \bmod 13 = 7$

$r = (g^k \bmod p) \bmod q$

$= (6^2 \bmod 27) \bmod 13$

$= \boxed{9} \bmod 13$

$s = k^{-1}(H + d \cdot r) \bmod q$

$= 2^{-1}(5 + 7 \cdot 9) \bmod 13$

$= 7 \cdot 68 \bmod 13$

$= 7 \cdot 3 \bmod 13$

$= \boxed{8}$

(b) Verify

$s' = 8^{-1} \bmod 13 = \boxed{5} \bmod 13$

$(8 \cdot 8^{-1} \bmod 13 = 1 \bmod 13)$

$r' = (\beta^{5r} g^{5'H'} \bmod p) \bmod q$ $(\beta = 6^n \bmod$

$= (\beta^{5\times 9} 6^{5\times 5} \bmod 27) \bmod 13$

check $r' \stackrel{?}{=} 9$

4. (a) In RSA, $S = M^d \bmod n$

(M: message)

So, S can be as large as $(n-1)$

the size of s, $|s| \approx |n| \approx 1024$ bits

(b) In ElGamal DS,

$r = \square \bmod p$, $S = \square \bmod p-1$.

So, $|r| = p-1 \cong 1024$ bits, $|s| = |p-2| \cong 1024$ bits

the size of signature is 2048 bits.

(c) In the DSS,

$r = \square \bmod q$, $S = \square \bmod q$.

$|r| = |s| = |q-1| \approx 160$ bits

so, size of signature is 320 bits.

6. input: (Tlen, K, k_1, $M = (M_1, \cdots, M_N)$, N=blocks)

K: AES key; $M = (M_1, \cdots, M_N) = M[1, \cdots, N]$

{

C[1] ← E_K(M[1])

i ← 2

while (i < N)

C[i] ← E_K(C[i-1] ⊕ M[i])

i ← i+1

C[N] ← E_K(C[N-1] ⊕ M[N] ⊕ k)

h ← selectLeft(C[N], Tlen)

return h.

}