1) Now consider the opposite problem: using an encryption algorithm to construct a one-way hash function. Consider using RSA with a known key. Then process a message consisting of a sequence of blocks as follows: Encrypt the first block, XOR the result with the second block and encrypt again, etc. Show that this scheme is not secure by solving the following problem.
Given a two-block message B1, B2, and its hash

$$RSAH(B1, B2) = RSA(RSA(B1) \oplus B2)$$

Given an arbitrary block C1, choose C2 so that RSAH(C1, C2) = RSAH(B1, B2). Thus, the hash function does not satisfy weak collision resistance.
Answer.
RSAH(C1, C2) = RSA(RSA(C1) ⊕ C2)
$= RSA(\ RSA(C1) \oplus RSA(C1) \oplus RSA(B1) \oplus B2\ )$
$= RSA(\ RSA(B1) \oplus B2\ )$
$= RSA(\ B1, B2\ )$
Therefore, choose C2 = RSA(C1) ⊕ RSA(B1) ⊕ B2

2) DSA specifies that if the signature generation process results in a value of s = 0, a new value of k should be generated and the signature should be recalculated. Why?
Answer.
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) Compute the signature of M="Hello!" using the specified methods, where H(W)=last 4 bits of SHA256(W) for a binary string W. Also, compute the corresponding public keys and verify correctness of the signatures.
H(W) =SHA256(W)=7= m
a) RSA: n=323=17x19, PR=(323, 7^{-1} mod 288).
PU=(d,n)=(7, 323)
Sign：$S=m^d \bmod n=H(W)^{247} \bmod 323 =216$
Verify:(H(W) ,S^e mod n)
$216^7 \bmod 323 = 7= H(W)$，Pass。
b) ElGamal: q=103, α=11, X_A=35.
PR=(q, α, X_A),(103,11,35)
$Y_A= \alpha^{X_A} \bmod q =11^{35} \bmod 103 = 101$
PU=(q, α , Y_A)=(103,11,101)

Sign：

Random choose k=3，1<k<q，gcd(k,q-1)=1

$S_1=\alpha^k$ mod q $=11^5$ mod 103 = 62

$S_2=k^{-1}(m- X_A S1)$ mod (q-1) = $5^{-1}(7- 35* 62)$ mod (102)=57

Verify: (α^m mod q , $Y_A^{S_1}$ $S_1^{S_2}$ mod q)

$\alpha^m = 11^7=86=101^{62} \times 62^{57}$ mod 103。Pass。

c) Schnorr: p=103, q=17, a=72, PR= (103, 17, 72, 10)

v $=a^{-s}$ mod p $=72^{-10}$ mod 103 = 66

PU=(p,q,a,v)=(103,17,72,66)

Sign:

x = a^r mod p =722 mod 103 = 34

e = H(M||X) =14

y=(r+se) mod q =(2+10x14) mod 17 = 6

Verify : (a^y v^e mod p , x)

a^y v^e mod p=$72^6 66^{14}$ mod 103 = 34=x，Pass

d) DSA: p=103, q=17, g=72, PR = (103, 17, 72, 7)

Random choose k=3

y=(g^x mod p) = 66

PU=(p,q,g,y)=(103,17,72,66)

Sign:

r =(g^k mod p)mod q =(72^3 mod 103) mod 17 =11

s =k^{-1} (H(m)+xr) mod q = 11

Verify: (r , (($g^{H(m)}y^r)^{(s\text{^-1 mod q})}$mod p)mod q)

(($g^{H(m)}y^r)^{(s\text{^-1 mod q})}$mod p)mod q =($72^7 66^{11}$)^{14} mod 103 mod 17 =11= r，Pass。

4) Use the DFT method to factor M=77 by choosing a=8, m=7, n=12. Use a tool, such as Matlab, to compute DFT. You need to show all steps of computation.

Step: 1.

Prepare a vector x = [0 1 2 … 2^{2m} – 1]。

Step: 2.

Compute $g_{a,M}(x)$

= [a^0 mod M , a^1 mod M , a^2 mod M , … $a^{2^{14}-1}$ mod M]

= [1 , 8 , 64 , 50 , 15 , 43 , ……]

Step: 3.

Compute and normalize $f = DFT(g_{a,M}(x))$

$f \approx$ [0.14 , 0 , 0 , 0 ,……] , f[410] ≈ 0.0167, f[819] ≈ 0.0439 , f[1229] ≈ 0.0240。

D=[0, 410, 819, 1229, 1638, 2458, 2867, 3277, 3686]

Step: 4.

Use “continued fraction” method to compute z1 , z2 , …, zr of denominators at most n-bit long for approximating d1/N, d2/N, …, dr/N within 1/2N。

d1/N= 410/4096=0.10009765625 ≈1/10。

∴ period s = 10 。(a^s mod M = 1)

Step: 5.

S is even and $a^{s/2}$ mod M ≠ ±1，then gcd($a^{s/2}$±1,M) = p or q。

gcd(a^5+1,M)=gcd(44,77)=11

gcd(a^5-1,M)=gcd(42,77)=7

∴ M=11 x 7