SOEN 321

Prob. 1 Consider a Rabin cryptosystem with p=7 and q=11. Find the four messages corresponding to c=58.

Solution steps:

cp= c mod p =2
cq= c mod q =3

mp= cp^{(p+1)/4} mod p = 4
mq= cq^{(q+1)/4} mod q = 3

To get m, we use CRT and solve
m = +/- mp mod p
m= +/- mq mod q

chrem([mp, mq],[p,q])=60
chrem([-mp, mq],[p,q])=38;
chrem([mp, -mq],[p,q])=39;
chrem([-mp, -mq],[p,q])=17;

Prob 2. Bob is a paranoid cryptographer who does not trust dedicated hash functions such as SHA1 and SHA-2. Bob decided to build his own hash function based on some ideas from number theory. More precisely, Bob decided to use the following hash function: $H(m)= m^2 \bmod n$, $n= p \times q$, where p and q are two large distinct primes. Does this hash function satisfy the one-wayness property? What about collision resistance? Explain.

Sol. Since p and q are secret, then finding the square root mod n is a hard problem. Thus this hash function satisfies the one-wayness property. On the other hand, H does not satisfy the weak/strong collision resistance property because for any m, -m would also have the same hash value, i.e., H(m)=H(-m).

Prob. 3 Consider a (4,3) Shamir secret sharing scheme with p=17. Show how the secret can be recovered from the following shares: (1,10), (2,16), and (3,2).

Ans.
Form 3 equations in 3 unknowns.
10=a0+a1+a2 mod 17
16=a0+2a1+4a2 mod 17
2=a0+3 a1+9a2 mod 17
=> a0=1, a1=2 and a2=7. Thus the secret =a0=1