**Problem 1**

29+28+27…+1 = 435

**Problem 2**

If M=(a||c) and M=(b||c) and M is a MAC function, then M(a) = M(b). If M(a) = M(b) then M(a||d) = M(b||d) for some block d. This is true because if a and b are equivalent under M, then chaining block d on to them will still keep them equivalent.

**Problem 3**

a. A large prime p and a g a primitive element in Zp\* are public values used by alice and bob to create a secret key. Alice chooses a random x in Zp\* and bob chooses a y in Zp\*. Alice sends bob gx mod p and bob sends alice gy mod p. They can then both compute the key k, =gxy mod p using the information that they exchange.

b. The hard problem that the security is based on is the discrete log problem.

c. a primitive element in the group Zp\* is an element which, when raised from 0-(q-1) can generate an entire group.

d. It is important that g is primitive modulo p in diffie hellman because it generates the whole group. If it is not primitive, the whole group is not generated, and can potentially be brute forced.

e. Using p=53 and g=23 to generate a key should NOT be used because 23 is not a primitive root of

**Problem 4**

37^57 mod 97 = 28 (Alice sends 28 to Bob)

(Bob sends Alice 84)

84^57 mod 97 = key =78

28^b mod 97 = 78, b=11

**Problem 5**

Apples and Bananas

**Problem 6**

PT 00101110010101

Key 11010001001111

CT 11111111011010

**Problem 7**

1. Perfect secrecy is when the cipher text reveals zero information about the underlying plaintext.
2. One Time Pad

**Problem 8**

1. To encrypt a message in RSA, a message M is padded using a sufficient padding scheme(OAEP) to produce *m*. The next step is to generate two large primes, p and q such that p and q are not close to each other. From this, the composite modulus n is calculated by n=p\*q. The next step is to get the Euler’s totient of n, denoted φ(n) by multiplying (p-1)\*(q-1)//GCD(p-1,q-1). So far we have p,q,n and φ(n).With this information a public key is generated by choosing a random number in the range (3, φ(n)). With *e* generated, we can deduce private key *e* -1 mod φ(n) with Euclid’s extended algorithm. So now with all the information we can encrypt padded message *m* as c(*m*) = *m e* mod n.
2. A trapdoor function is a function that is hard to reverse without “trapdoor” information, but with the trapdoor information the reversal is easy. In the case of RSA, n is the trapdoor because factoring n is hard, unless you have both p and q. RSA is implemented on this principle.
3. 445. 1335 is a product of three primes, and 503 is a prime. An modulus for RSA must be a product of two primes.

**Problem 9**

1. The Chinese remainder theorem states that you can compute the inverse given x mod p and x mod q , so you can reconstruct x.
2. 107 = 89(1) + 18

89 = 18(4) + 17

18 = 17(1) + 1

1 = 18 – 17

= 18 – (89 + 18(-4)

= 18(5) + 89(-1)

= (107-89)(5) +89(-1)

= 107(5) + 89(-6)

= q-1 = 5

x=(((3-5)(5mod89))mod89)\*107+5

= -10 mod 89 \*107 + 5

= 79\*107+5

= 8458

**Problem 10**

φ(n) = (p-1)(q-1) = 6160

3\*e-1=1mod 6160

6160 = 3(2053) + 1

1 = 6160 + 3(-2053)

e-1 = -2053 +6160 = 4107

d= 4107

s = md mod n

= 54164107 mod (71\*89)

= 1876

**Problem 11**

Cd = m mod n

41204107 mod (71\*89) = 333

m = 333

Check

3333 mod (71\*89) = 4120

**Problem 12**

1. No because 42 mod 19 is not in the group.
2. Yes, because it satisfies all the conditions to form a group under multiplication.(Identity, associativity,…)

**Problem 13**

VIIEILLGX

**Problem 14**

1491823 = 180(8287) + 163

180 = 163 + 17

163 = 17(9) + 10

17 = 10 + 7

10 = 7 + 3

7 = 3(2) + 1

1 =7 – 3(2)

= 7(3) + 10(-2)

= 17(3) + 10(-5)

= 17(48) + 163(-5)

= 180(48) + 163(-53)

= 1491823(-53) + 180(439259)

180-1 = 439259 mod 1491823