Asymmetrical Cryptography/Public Key Cryptography

Digital Signing  
RSA Algorithm

Symmetric Cryptography – same key for encryption and decryption

C=E(K,P), P=D(K,C)  
-Keys need to be exchanged secretly  
-Great many keys may need to be exchanged  
  
2 2(2-1)/2 1  
100 4950 4950

Asymmetric Cryptography-Public Key Cryptography  
Encryption/decryption requires a pair of keys

Key Generator Algorithm  
-Public key Kpublic  
-Pri­­­vate key Kprivate

Private keys cannot feasibly be inferred from the public key  
-Most systems it can be done, but would require excessive power (semantic security)  
-However, key pair must be generated without using excessive computing power  
-Mathematical “trap door” function

C=E(KPUB,A,E(KPRIV,B,P))

RSA – Public key: Kpub=(n,e)  
 Private key:Kpriv(n,d)  
e= public key index  
d= private key index  
n= modulus   
Plaintext is converted to an integer P mod n  
Ciphertext represented by integer C mod n  
Number of unique messages possible to encrypt is n

Encryption: E(e,n,P) = Pe mod n  
Decryption: D(d,n,C) = Cd mod n

(Pe mod n)d mod n = P  
(Cd mod n)e mod n = C

Euler’s Totient Function

Φ(n)  
Φ(4) = 2  
If p is prime, Φ(p)=p-1  
Φ(x\*y) = Φ(x) \* Φ(y)

If n has prime factors of p and q then:  
Φ(p\*q) = (p-1)(q-1)

p=5, q=7, n=5\*7  
Φ(n)= (5-1)(7-1) = 24 = N

If gcd(a,n) = 1 then aΦ(n) mod n = 1

mΦ(n) mod n = 1 => [mΦ(n)]k mod n = 1k = 1

mk.\*Φ(n) mod n = 1 => mk.\*Φ(n)+1 mod n = m

Choose 2 prime numbers, p and q  
P and Q should be large (100 digits each)  
Limited sieve followed primality testing  
m=p\*q  
N= Φ(p\*q) – (p-1)(q-1)  
Choose e which is relatively prime with N

Retain n,e,d  
Delete p,q,N  
Plaintext P => C=Pemod n

P = 11, Q = 13

n = pq =11\*13 = 143  
N = (p-1)(q-1) = 10\*12 = 120  
e = 17  
d => 17\*d mod 120 = 1  
d => Euclidean algorithm  
120:17 = 7 120-7\*17 = 1  
0-7\*1 = -7  
-7 mod 120 = 113   
d = 113  
C=Pemod n C=P17mod 143  
P=Cdmod n P=C113mod 143

q=5, p=11  
n= 5\*11=55  
N=4\*10=40  
e=17  
d=17\*d mod40 = 1  
40:17 = 2 40-17\*2 = 6  
17:6 = 2 17-6\*2 = 5  
6:5 = 1 6-1\*5=1

0-2x1 = -2  
1-2x-2 = 5  
-2-1x5 =-7  
-7 mod 40 = 33  
d = 33  
C=P17mod 55  
P=C33mod 55