Jon Scott
CPE 321 - 01
Lab 2
May 05, 2017

S	P	I	E	A
B	C	D	F	G
H	K	L	M	N
O	Q	R	T	U
V	W	X	Y	Z

1) Ciphertext: OM EU P A DQ FY VT OZ S F IY AM NZ IU L D UN EP MU
    a) Key: SPIES
    b) Plaintext
        i) THATSECRETYOUVEBEXENGAURDINGISNT
        ii) That secret you've been guarding isn't
2) Assuming that we are not concerned with the problem of key exchange, each user could use a unique key to communicate with one other user. So if we can model the problem as a complete graph with m vertices and K edges.
    a) From graph theory, we know that the number of edges for a complete graph with m vertices can be written as
        i) $K = m (m - 1) / 2$
3) In a public key cryptosystem, each user uses two keys: a public and a private key. Therefore the number of K keys in such a system can be written as
    a) $K = 2 * m$
    b) Note: Each user would be able to communicate with a single other user without the other eavesdropping, but the user that are communicating cannot be certain with whom they are talking to.
4) The problem of interest here is nonrepudiation. We need to make use of digital signatures, time stamps, and cryptographic hashes in order to prove the identities of two parties. Suppose investor A wants to endorse a message. First, he should add a timestamp to his message and then run the document through a cryptographic hash. Then he should encrypt the result of the hash with his private key. This hashing of the message with a timestamp, in combination with the encryption of his private key, ensures that it would be

computationally infeasible for an attacker to spoof the investor and protects against repeat attacks. The investor and stockbroker should also choose to trust a third party, whom can issue certificates of authenticity to both parties. When the investor sends the message to the stockbroker, he should send the following:

$$\{m \,||\, \{f(m)\}K_{DA} \,||\, C_{authority}\}K_{EB}$$

m: message

f ( ): is the cryptographic hash

$C_{authority}$: the certificate from the trusted third party.

K_{DA}: the investor's private key

K_{EB} : the stockbroker's public key

When the stockbroker receives the message, he should send a message a reply using a similar format as above, confirming the recipient of the first message, and requesting permission to continue. Then, the investor can send authorization to proceed.

By asking the investor to confirm a transaction, both the investor and stockbroker are able to keep records of the conversation with the certified identity of the other.

As a final, unrealistic option, the two groups could of course decide not to do business with shady groups or individuals.

5) RSA encryption

n = 55 (Modulus)

e = 7 (Public Key)

M = 10 (Plaintext Message)

C (Ciphertext Message)

$C = M^e \bmod n$

$C = 10 \bmod 55$

C = 10

6) RSA decryption

$\phi(n)$ (Totient Function)

n = 55 (Modulus)

e = 7 (Public Key)

C = 35

Find p and q (two prime numbers) and d (private key) in order to get P (plaintext)

Important Equations

Equation 1	$n = pq$
Equation 2	$\phi(n) = (p - 1)(q-1)$
Equation 3	$ed = 1 \bmod \phi(n)$

We need to find the primes used to get the modulus.

Possible Primes (List of primes less than 55)

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53

So we do some educated guessing to solve equation #1. Divide the modulus by the possible primes. The correct prime will have no remainder.

55 / 2 = 27.5 (NOT THE ANSWER)

55 / 3 = 18.33333 (NOT THE ANSWER)

55 / 5 = 11 (We found p and q)

Therefore p = 5 and q = 11

Now we solve the totient of the modulus (equation 2) using p and q

$\phi(n) = (p - 1)(q-1)$

$\phi(55) = (5 - 1)(11-1)$

$\phi(55) = 40$

Substitute the totient into equation 3 in order to find the private key

$ed = 1 \bmod \phi(n)$

$7d = 1 \bmod 40$

Using some more educated guessing…

Use the model:

$7d = (40 * x) + 1$

1. If x = 1, 7d = 41
    a. d = 41/7 = 5.857 (Not the answer)
2. If x = 2, 7d = 81
    a. d = 81/7 = 11.571 (Not the answer)
3. If x = 3, 7d = 121
    a. d = 121 / 7 = 17.285 (Not the answer)
4. If x = 4, 7d = 161
    a. d = 161 / 7 = 23 (This is the answer because there is no remainder!)

Therefore, d = 23

So,

$P = C^d \bmod n$

$P = 35^{23} \bmod 55$

$P = 30 \bmod 55$

$P = 30$