## Announcements:

· Miltern next Monday 7/12 @ 8pm -see Piazza for logistics

public key privak key

(N, e)

Alive > Bob! E(x)= x (red N)

\* N= pe for P, e prime

\* R = caprime to (p-1)(e-1)

\* Red = 1 (red (p-1)(e-1))

Bob decrypt: D(ECX)):(Xe)d (not N)

= x (med N)

RSA Warm-Up

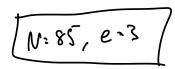
Consider an RSA scheme with modulus N = pq, where p and q are distinct prime numbers larger than 3.

(a) What is wrong with using the exponent e=2 in an RSA public key? Need gcd(e, (p-1)(2-1))=1, but p-1  $\neq q-1$  are even so gcd (2, cp-1)(q-1) = 2. - e should never be even

(b) Recall that e must be relatively prime to p-1 and q-1. Find a condition on p and q such that e = 3 is a valid exponent.

e = 3 is a valid exponent. -p-1 & g-1 can't be multiples of 3 So p, q must be of the form 3k+2

(c) Now suppose that p = 5, q = 17, and e = 3. What is the public key?



(d) What is the private key?  $34 = 1 \pmod{64}$ 



(e) Alice wants to send a message x = 10 to Bob. What is the encrypted message E(x) she sends using the public key?

(f) Suppose Bob receives the message 
$$y = 24$$
 from Alice. What equation would be use to decrypt the message? What is the decrypted message? FLT:  $a = (nod p)$ 
 $By CRT:$ 
 $a^3 = x \cdot (nod 5)$ 
 $a^3 = x \cdot (nod 5)$ 

$$24^{43} = (-1)^{\frac{43}{2}} - 1 = 4 \pmod{5}$$

$$24^{3} = 7^{11} = (7^{2})^{5} \cdot 7 = (-1)(-1) \cdot 7 = 14 \pmod{7}$$

$$24^{3} = 7^{11} = (7^{2})^{5} \cdot 7 = (-1)(-1) \cdot 7 = 14 \pmod{7}$$

FLT

$$24^{3} = 4 \pmod{5}$$
 $24^{3} = 14 \pmod{17}$ 
 $24^{3} = 14 \pmod{17}$ 

$$24^{43} = 4(51) + 14(35)$$
 (mad 85)  
= 204 + 13.5 (mad 85)

$$= 34+65$$
 (nod 85)  
 $= 99$  (mod 85)  
 $= 14$  (mod 85)

## 2 RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like  $(N_1, e), \ldots, (N_k, e)$  where no two  $N_i$ 's are the same. Assume that the message is x such that  $0 \le x < N_i$  for every i.

(a) Suppose Eve sees the public keys  $(p_1q_1,7)$  and  $(p_1q_2,7)$  as well as the corresponding transmissions. Can Eve use this knowledge to break the encryption? If so, how? Assume that Eve cannot compute prime factors efficiently. Think of  $p_1,q_1,q_2$  as massive 1024-bit numbers. Assume  $p_1,q_1,q_2$  are all distinct and are valid primes for RSA to be carried out.

Yes, Eve knows p, are the same, so gcd(P121,P122)=P,
Now Eve can find q1, q2 by dividing Ni/P,

(b) The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now. Eve sees kevs  $(p_1q_1.3)$ .  $(p_2q_2.3)$ . and  $(p_3q_3.3)$  along with their transmissions. Argue why Eve cannot break the encryption in the same way as above. Assume  $p_1, p_2, p_3, q_1, q_2, q_3$  are all distinct and are valid primes for RSA to be carried out.

Now, none of the Ni's have common factors so Fue cannot use the GCD to divide out any Ni's.

(c) Let's say the secret x was not changed (e = 3), so they used the same public keys as before, but did not transmit different messages. How can Eve figure out x?

Eve sees  $x^3$  mad  $N_1$ ,  $x^3$  mad  $N_2$ ,  $x^3$  mad  $N_3$ , Since  $N_1$ 's are relatively prime, Eve can use CRT to find  $x^3$  (mad  $N_1N_2N_3$ ). Since  $x < N_1 \ \forall i$ ,  $x^3 < N_1 \ N_2 \ N_3$  so Eve can find x.

## 3 RSA for Concert Tickets

Alice wants to tell Bob her concert ticket number, m, which is an integer between 0 and 100 inclusive. She wants to tell Bob over an insecure channel that Eve can listen in on, but Alice does not want Eve to know her ticket number.

(a) Bob announces his public key (N = pq, e), where N is large (512 bits). Alice encrypts her message using RSA. Eve sees the encrypted message, and figures out what Alice's ticket number

is. now did she do it?

only (of possible values for Alice's fizhet number, Eve can try doing me (med N) for me \( \frac{20}{1}, \frac{2}{2}, \ldots, \cos\} \) and see which in works.

(b) Alice decides to be a bit more elaborate. She picks a random number r that is 256 bits long, so that it is too hard to guess. She encrypts that and sends it to Bob, and also computes rm, encrypts that, and sends it to Bob. Eve is aware of what Alice did, but does not know the value of r. How can she figure out m?

Alice sends  $x = re \pmod N$  &  $y = (rm)^e = xm^e \pmod N$ Eve can find  $x^{-1} \pmod N$  & multiply this by y getting  $m^e$  (mad N). Now use part a)