Discussion 3C

CS 70, Summer 2024

1 RSA Warm-Up

Consider an RSA scheme with a modulus $N = pq$ for p, q distinct prime numbers larger than 3.

(a) Explain why we cannot use an exponent of $e = 2$.

(b) Find a condition on p and q such that $e = 3$ is a valid exponent.

(c) For this part and the following parts, suppose that $p = 5$, $q = 17$, and $e = 3$. Find the public key for this RSA scheme.

(d) Find the private key for the RSA scheme.

(e) Suppose Anja wants to send Benito the message $x = 10$ using this RSA scheme. Find the encrypted message $E(x)$ that Anja will send to Benito.

(f) Suppose that under this RSA scheme, Benito receives the message encrypted message $y = 19$ from Anja. Find the original message that Anja sent.

2 RSA with Multiple Keys

A secret society uses the RSA scheme to encrypt their secret messages. For each $i \in \mathbb{N}$, let (N_i, e_i) be the public key they use for their i^{th} secret message.

Ewen is listening in on their communications and is trying to deicpher their secret messages.

(a) Ewen figures out that the secret society is using the same prime p to generate their keys. That is, their moduli are of the form $N_1 = pq_1, N_2 = pq_2, \ldots$, where $p, q_1, q_2, \ldots$ are distinct primes.

Ewen sees two public keys (N_1, e_1) and (N_2, e_2) along with their corresponding encrypted messages y_1 and y_2. Explain how Ewen can use her knowledge of the key generation process to break the encryption.

(b) Having wised up to Ewen, the secret society changes their scheme. They generate the public keys with distinct primes, so their moduli are of the form $N_1 = p_1 q_2, N_2 = p_2 q_2, \ldots$, where $p_1, q_1, p_2, q_2, \ldots$ are distinct primes. However, now they use the same exponent e in all their transmissions.

On top of that, Ewen has figured out that every transmission includes a secret word x that the secret society uses for their secret purposes. Suppose Ewen knows that x is small with respect to the moduli; that is, $x < N_i$ for each $i \in \mathbb{N}$. Ewen sees two public keys $(N_1, 2)$ and $(N_2, 2)$, along with the corresponding encryptions y_1 and y_2 of the secret word x. Explain how Ewen can break the encryption to figure out their secret word x.

3 Concert Tickets

Akemi and Burut are going to a concert. Akemi wants to privately tell Burut their concert ticket number $x \in \{0, \dots, 100\}$, but their communication channel is insecure and Eileen can see their transmissions.

(a) Bhurut announces his public key (N, e), where N is large. Akemi uses the RSA scheme to send Bhurut their ticket number x. Eileen sees Akemi's encrypted message y. Explain how Eileen can figure out Akemi's ticket number x.

(b) Akemi decides to be a bit more elaborate. They pick a number r which is coprime to N. They encrypt r and send it to Bhurut. Then they compute rx, encrypts it, and sends it to Bhurut.

Eileen sees Akemi's encrypted messages y_1 and y_2. Eileen is aware of what Akemi's process, but she doesn't know the value of r that Akemi used. Explain how Eileen can figure out Akemi's ticket number x.