UNIVERSITY OF WATERLOO

The RSA Encryption Scheme

The CENTRE for EDUCATION in MATHEMATICS and COMPUTING

Suppose Alice wants her friends to encrypt email messages before sending them to her. Computers represent text as long numbers (01 for "A", 02 for "B" and so on), so an email message is just a very big number. The RSA Encryption Scheme is often used to encrypt and then decrypt electronic communications.

General

Alice's Setup:

- Chooses two prime numbers.
- Calculates the product $n = pq$.
- Calculates $m = (p-1)(q-1)$.
- Chooses numbers e and d so that ed has a remainder of 1 when divided by m.
- Publishes her public key (n, e).

Bob encrypts a message M for Alice:

- Finds Alice's public key (n, e).
- Finds the remainder C when M^e is divided by n.
- Sends ciphertext C to Alice.

Alice receives and decrypts ciphertext C:

- Uses her private key (n, d).
- Finds remainder R when C^d is divided by n.
- R matches the message M that Bob wanted to send to Alice!

Example

Alice's Setup:

- $p = 11$ and $q = 3$.
- $n = pq = 11 \times 3 = 33$.
- $m = (p-1)(q-1) = 10 \times 2 = 20$.
- If $e = 3$ and $d = 7$, then $ed = 21$ has a remainder of 1 when divided by $m = 20$.
- Publish $(n, e) = (33, 3)$.

Bob encrypts message $M = 14$:

- $(n, e) = (33, 3)$.
- When $14^3 = 2744$ is divided by 33, the remainder is $C = 5$.
- Sends ciphertext $C = 5$ to Alice.

Alice decrypts ciphertext $C = 5$:

- $(n, d) = (33, 7)$.
- When $5^7 = 78125$ is divided by 33, the remainder is $R = 14$.
- $R = 14 = M$, the original message from Bob!

Questions

1. Callie wants to send the message $M = 13$ to Alice. Using Alice's public and private keys, calculate the ciphertext C, and the value for R when Alice recovers the message.

2. Dexter wants to set up his own public and private keys. He chooses $p = 23$ and $q = 19$ with $e = 283$. Find d so that ed has a remainder of 1 when divided by $(p-1)(q-1)$.

Connection to the Real World

When your internet browser shows a URL beginning with https, the RSA Encryption Scheme is being used to protect your privacy. For example, if you log in to Facebook, your computer plays the role of Alice and the Facebook server plays the role of Bob, encrypting and decrypting the information passed back and forth. In practice, the primes p and q are chosen to be very big numbers.

Mathematics is the foundation of modern encryption.

Solution:

1. **Callie encrypts message $M = 13$:**

   - Alice's public key is $(n, e) = (33, 3)$.
   - When $M^e = 13^3 = 2197$ is divided by 33, the remainder is $C = 19$.
   - Callie sends to Alice ciphertext $C = 19$.

   Alice receives and decrypts ciphertext $C = 19$:

   - Alice uses her private key $(n, d) = (33, 7)$.
   - When $19^7 = 893,871,739$ is divided by 33, the remainder is $R = 13$.
   - $R = 13 = M$, the original message from Callie!

2. With $p = 23, q = 19$, we have $m = (p - 1)(q - 1) = 22(18) = 396$.
   We want to find d so that $ed = 283d$ has a remainder of 1 when divided by $m = 396$. One way to do this is by simple trial and error, increasing the value of d until $283d$ divided by 396 leaves a remainder of 1.

d	$283d$	Remainder when $283d$ is divided by 396
1	283	283
2	566	170
3	849	57
4	1132	340
5	1415	227
6	1698	114
7	1981	1

   We see that $d = 7$ works; that is $ed = 283 \times 7 = 1981$ leaves a remainder of 1 when divided by 396.

   In general, trial and error could take a very long time, as the value of d could be a big number. Instead, an ancient technique called Euclid's Algorithm can be used to find d in the linear Diophantine equation $283d + 396y = 1$.