Carmen's Core Concepts (Math 135)

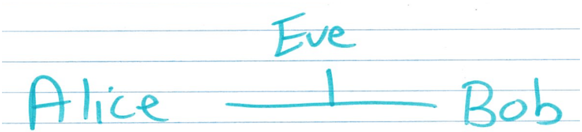
Carmen Bruni

University of Waterloo

Week 9 Part 1 - RSA

Exponentiation Ciphers

Suppose Alice and Bob want to share a message but there is an eavesdropper (Eve) watching their communications.



Exponentiation Ciphers

- In an exponentiation cipher, Alice chooses a (large) prime p and an e satisfying

$$1 < e < (p-1) \qquad \text{and} \qquad \gcd(e, p-1) = 1.$$

Exponentiation Ciphers

- In an exponentiation cipher, Alice chooses a (large) prime p and an e satisfying

$$1 < e < (p-1) \qquad \text{and} \qquad \gcd(e, p-1) = 1.$$

- Alice then makes the pair (e, p) public and computes her private key d satisfying

$$1 < d < (p-1) \qquad \text{and} \qquad ed \equiv 1 \pmod{p-1}$$

which can be done quickly using the Euclidean Algorithm (the inverse condition above is why we required that $\gcd(e, p-1)$).

Exponentiation Ciphers

- In an exponentiation cipher, Alice chooses a (large) prime p and an e satisfying

$$1 < e < (p-1) \qquad \text{and} \qquad \gcd(e, p-1) = 1.$$

- Alice then makes the pair (e, p) public and computes her private key d satisfying

$$1 < d < (p-1) \qquad \text{and} \qquad ed \equiv 1 \mod p-1$$

  which can be done quickly using the Euclidean Algorithm (the inverse condition above is why we required that $\gcd(e, p-1)$).
- To send a message M to Alice, an integer between 0 and $p-1$ inclusive, Bob computes a ciphertext (encrypted message) C satisfying

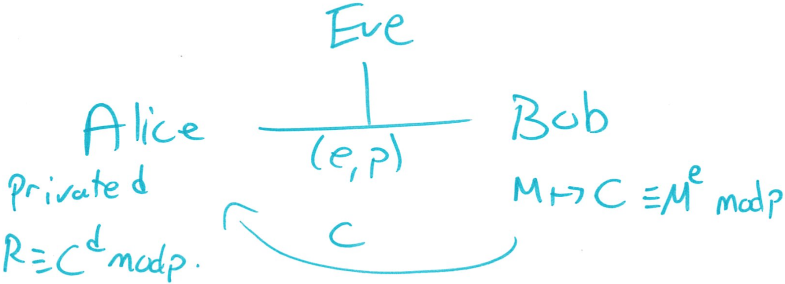
$$0 \le C < p \qquad \text{and} \qquad C \equiv M^e \mod p.$$

  Bob then sends C to Alice.

Exponentiation Ciphers

- In an exponentiation cipher, Alice chooses a (large) prime p and an e satisfying
$$1 < e < (p-1) \qquad \text{and} \qquad \gcd(e, p-1) = 1.$$
- Alice then makes the pair (e, p) public and computes her private key d satisfying
$$1 < d < (p-1) \qquad \text{and} \qquad ed \equiv 1 \mod p-1$$
which can be done quickly using the Euclidean Algorithm (the inverse condition above is why we required that $\gcd(e, p-1)$).
- To send a message M to Alice, an integer between 0 and $p-1$ inclusive, Bob computes a ciphertext (encrypted message) C satisfying
$$0 \leq C < p \qquad \text{and} \qquad C \equiv M^e \mod p.$$
Bob then sends C to Alice.
- Alice then computes $R \equiv C^d \mod p$ with $0 \leq R < p$.

Exponentiation Ciphers Diagram



Exponentiation Ciphers Main Proposition

Proposition: $R \equiv M \mod p$.

Exponentiation Ciphers Main Proposition

Proposition: $R \equiv M \mod p$.

Proof: If $p \mid M$, then all of M, C and R are 0 and the claim follows. So we assume that $p \nmid M$. Recall that $ed \equiv 1 \mod p-1$ and so we have that there exists an integer k such that $ed = 1 + k(p-1)$. Using this, we have

$$\begin{aligned} R &\equiv C^d \mod p \\ &\equiv (M^e)^d \mod p \quad \text{by definition of } C \\ &\equiv M^{ed} \mod p \\ &\equiv M \mod p \qquad \text{Corollary to F}\ell\text{T since } ed \equiv 1 \mod p-1. \end{aligned}$$

as required ■

Corollary: $R = M$

The Good, The Bad and The Ugly

The good news is that this scheme works. However, Eve can compute d just as easily as Alice! Eve knows p, hence knows $p - 1$ and can use the Euclidean algorithm to compute d just like Alice. This means our scheme is not secure. To rectify this problem, we include information about two primes.

RSA

- Alice chooses two (large) distinct primes p and q, computes $n = pq$ and selects any e satisfying

$$1 < e < (p-1)(q-1) \qquad \text{and} \qquad \gcd(e,(p-1)(q-1)) = 1$$

RSA

- Alice chooses two (large) distinct primes p and q, computes $n = pq$ and selects any e satisfying

  $$1 < e < (p-1)(q-1) \qquad \text{and} \qquad \gcd(e, (p-1)(q-1)) = 1$$

- Alice then makes the pair (e, n) public and compute her private key d satisfying

  $$1 < d < (p-1)(q-1) \qquad \text{and} \qquad ed \equiv 1 \mod (p-1)(q-1)$$

  again which can be done quickly using the Euclidean Algorithm (Alice knows p and q and hence knows $(p-1)(q-1)$).

RSA

- Alice chooses two (large) distinct primes p and q, computes $n = pq$ and selects any e satisfying

  $$1 < e < (p-1)(q-1) \qquad \text{and} \qquad \gcd(e, (p-1)(q-1)) = 1$$

- Alice then makes the pair (e, n) public and compute her private key d satisfying

  $$1 < d < (p-1)(q-1) \qquad \text{and} \qquad ed \equiv 1 \mod (p-1)(q-1)$$

  again which can be done quickly using the Euclidean Algorithm (Alice knows p and q and hence knows $(p-1)(q-1)$).
- To send a message M to Alice, an integer between 0 and $n-1$ inclusive, Bob computes a ciphertext C satisfying

  $$0 \le C < pq \qquad \text{and} \qquad C \equiv M^e \mod pq.$$

RSA

- Alice chooses two (large) distinct primes p and q, computes $n = pq$ and selects any e satisfying

$$1 < e < (p-1)(q-1) \qquad \text{and} \qquad \gcd(e, (p-1)(q-1)) = 1$$

- Alice then makes the pair (e, n) public and compute her private key d satisfying

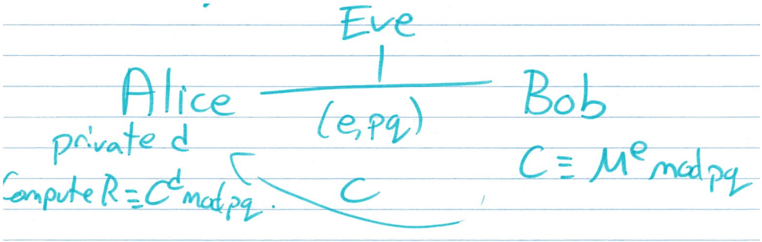
$$1 < d < (p-1)(q-1) \qquad \text{and} \qquad ed \equiv 1 \mod (p-1)(q-1)$$

  again which can be done quickly using the Euclidean Algorithm (Alice knows p and q and hence knows $(p-1)(q-1)$).
- To send a message M to Alice, an integer between 0 and $n - 1$ inclusive, Bob computes a ciphertext C satisfying

$$0 \leq C < pq \qquad \text{and} \qquad C \equiv M^e \mod pq.$$

- Bob then sends C to Alice. Alice then computes $R \equiv C^d \mod pq$ with $0 \leq R < pq$.

RSA Diagram



RSA Main Theorem

Proposition: $R = M$.

Proof: Since $ed \equiv 1 \mod (p-1)(q-1)$, transitivity of divisibility tells us that

$$ed \equiv 1 \mod p-1 \qquad \text{and} \qquad ed \equiv 1 \mod q-1.$$

Since $\gcd(ed, (p-1)(q-1)) = 1$, GCD Prime Factorization tells us that $\gcd(ed, p-1) = 1$ and that $\gcd(ed, q-1) = 1$. Next, as $C \equiv M^e \mod pq$, Splitting the Modulus states that

$$C \equiv M^e \mod p \qquad \text{and} \qquad C \equiv M^e \mod q$$

Similarly, by Splitting the Modulus, we have

$$R \equiv C^d \mod p \qquad \text{and} \qquad R \equiv C^d \mod q.$$

By the previous proposition applied twice, we have that

$$R \equiv M \mod p \qquad \text{and} \qquad R \equiv M \mod q.$$

RSA Main Theorem

Proposition: $R = M$.

Proof: (Continued) By the previous proposition applied twice, we have that

$$R \equiv M \mod p \qquad \text{and} \qquad R \equiv M \mod q.$$

Now, an application of the Chinese Remainder Theorem (or Splitting the Modulus), valid since p and q are distinct, gives us that $R \equiv M \mod pq$. Recalling that $0 \leq R, M < pq$, we see that $R = M$. ■

Security and Food for Thought

- Is this scheme more secure? Can Eve compute d? If Eve can compute $(p-1)(q-1)$ then Eve could break RSA. To compute this value given only n (which recall is pq), Eve would need to factor n. Factoring n is hard. Eve could also break RSA if she could solve the problem of computing M given $M^e \mod n$.
- Let φ be the Euler Phi Function. Note $\varphi(n) = (p-1)(q-1)$ when $n = pq$ is a product of distinct primes.
- How does Alice choose primes p and q?
- What if Eve wasn't just a passive eavesdropper? What if Eve could change the public key information before it reaches Bob? (This involves using certificates).
- What are some advantages of RSA? (Believed to be secure, uses the same hardware for encryption and decryption, computations can be done quickly).

An Example

Let $p = 2$, $q = 11$ and $e = 3$

1. Compute n, $\phi(n)$ and d.
2. Compute $C \equiv M^e \mod n$ when $M = 8$.
3. Compute $R \equiv C^d \mod n$ when $C = 6$.

An Example

Let $p = 2$, $q = 11$ and $e = 3$

1. Compute n, $\phi(n)$ and d.
2. Compute $C \equiv M^e \mod n$ when $M = 8$.
3. Compute $R \equiv C^d \mod n$ when $C = 6$.

Solution:

1. Note $n = 22$, $\phi(n) = (2-1)(11-1) = 10$ and $3d \equiv 1 \mod 10$. Multiplying by 7 gives $d \equiv 7 \mod 10$. Hence $d = 7$.
2. Note that

$$\begin{aligned} C \equiv M^e &\equiv 8^3 \mod 22 \\ &\equiv 8 \cdot 64 \mod 22 \\ &\equiv 8 \cdot (-2) \mod 22 \\ &\equiv -16 \mod 22 \\ &\equiv 6 \mod 22 \end{aligned}$$

An Example Finished

Let $p = 2$, $q = 11$ and $e = 3$

1. Compute n, $\phi(n)$ and d. ($n = 22$, $\phi(n) = 10$, $d = 7$)
2. Compute $C \equiv M^e \mod n$ when $M = 8$ ($C = 6$).
3. Compute $R \equiv C^d \mod n$ when $C = 6$.

An Example Finished

Let $p = 2$, $q = 11$ and $e = 3$

1. Compute n, $\phi(n)$ and d. $(n = 22,\ \phi(n) = 10,\ d = 7)$
2. Compute $C \equiv M^e \mod n$ when $M = 8$ $(C = 6)$.
3. Compute $R \equiv C^d \mod n$ when $C = 6$.

Solution: (of last part) The quick way to solve this is to recall the RSA theorem and hence $M = 8$. The long way is to do the following:

$$\begin{aligned} R \equiv C^d & \equiv 6^7 \mod 22 \\ \equiv 6 \cdot (6^3)^2 & \equiv 6 \cdot (216)^2 \mod 22 \\ \equiv 6 \cdot (-4)^2 & \equiv 6 \cdot 16 \mod 22 \\ \equiv 6 \cdot (-6) & \equiv -36 \mod 22 \\ \equiv 8 \mod 22 & \end{aligned}$$