Algorithmic Number Theory and Cryptography
(CS 303)

Modular Arithmetic and the RSA Public Key Cryptosystem

Jeremy R. Johnson
Introduction

- Objective: To understand what a public key cryptosystem is and how the RSA algorithm works. To review the number theory behind the RSA algorithm.

  - Public Key Cryptosystems
  - RSA Algorithm
  - Modular Arithmetic
  - Euler’s Identity
  - Chinese Remainder Theorem

References: Rivest, Shamir, Adelman.
Modular Arithmetic ($\mathbb{Z}_n$)

Definition: $a \equiv b \pmod{n} \iff n \mid (b - a)$

Alternatively, $a = qn + b$

Properties (equivalence relation)

– $a \equiv a \pmod{n}$ [Reflexive]
– $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ [Symmetric]
– $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ [Transitive]

Definition: An equivalence class mod $n$

$[a] = \{ x: x \equiv a \pmod{n} \} = \{ a + qn \mid q \in \mathbb{Z} \}$
Modular Arithmetic ($\mathbb{Z}_n$)

It is possible to perform arithmetic with equivalence classes mod $n$.

- $[a] + [b] = [a+b]$  
- $[a] \cdot [b] = [a\cdot b]$  

In order for this to make sense, you must get the same answer (equivalence) class independent of the choice of $a$ and $b$. In other words, if you replace $a$ and $b$ by numbers equivalent to $a$ or $b$ mod $n$ you end of with the sum/product being in the same equivalence class.

$$a_1 \equiv a_2 \pmod{n} \text{ and } b_1 \equiv b_2 \pmod{n} \Rightarrow a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$$
$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{n}$$

$$(a + q_1 n) + (b + q_2 n) = a + b + (q_1 + q_2)n$$
$$(a + q_1 n) \cdot (b + q_2 n) = a \cdot b + (b\cdot q_1 + a\cdot q_2 + q_1 \cdot q_2)n$$
Representation of $\mathbb{Z}_n$

The equivalence classes $[a] \mod n$, are typically represented by the representatives $a$.

- **Positive Representation**: Choose the smallest positive integer in the class $[a]$ then the representation is $\{0, 1, \ldots, n-1\}$.

- **Symmetric Representation**: Choose the integer with the smallest absolute value in the class $[a]$. The representation is $\{-\lceil (n-1)/2 \rceil, \ldots, \lceil n/2 \rceil \}$. When $n$ is even, choose the positive representative with absolute value $n/2$.
- **E.G.** $\mathbb{Z}_6 = \{-2, -1, 0, 1, 2, 3\}$, $\mathbb{Z}_5 = \{-2, -1, 0, 1, 2\}.$
Modular Inverses

Definition: $x$ is the inverse of $a$ mod $n$, if $ax \equiv 1 \pmod{n}$

The equation $ax \equiv 1 \pmod{n}$ has a solution iff $\gcd(a,n) = 1$.

By the Extended Euclidean Algorithm, there exist $x$ and $y$ such that $ax + ny = \gcd(a,n)$. When $\gcd(a,n) = 1$, we get $ax + ny = 1$. Taking this equation mod $n$, we see that $ax \equiv 1 \pmod{n}$

By taking the equation mod $n$, we mean applying the mod $n$ homomorphism: $\phi_m : \mathbb{Z} \rightarrow \mathbb{Z}_m$, which maps the integer $a$ to the equivalence class $[a]$. This mapping preserves sums and products. I.E.

$\phi_m(a+b) = \phi_m(a) + \phi_m(b), \phi_m(a*b) = \phi_m(a) * \phi_m(b)$
Fermat’s Theorem

Theorem: If \( a \neq 0 \in \mathbb{Z}_p \), then \( a^{p-1} \equiv 1 \pmod{p} \). More generally, if \( a \in \mathbb{Z}_p \), then \( a^p \equiv a \pmod{p} \).

Proof: Assume that \( a \neq 0 \in \mathbb{Z}_p \). Then
\[
a \ast 2a \ast \ldots \ast (p-1)a = (p-1)! \ast a^{p-1}
\]

Also, since \( a^i \equiv a^j \pmod{p} \Rightarrow i \equiv j \pmod{p} \), the numbers \( a, 2a, \ldots, (p-1)a \) are distinct elements of \( \mathbb{Z}_p \). Therefore they are equal to \( 1, 2, \ldots, (p-1) \) and their product is equal to \( (p-1)! \pmod{p} \). This implies that

\[
(p-1)! \ast a^{p-1} \equiv (p-1)! \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}.
\]
Euler phi function

• Definition: \( \phi(n) = \#\{a: 0 < a < n \text{ and } \gcd(a,n) = 1\} \)

• Properties:
  - \( \phi(p) = p-1, \text{ for prime } p. \)
  - \( \phi(p^e) = (p-1)p^{(e-1)} \)
  - \( \phi(mn) = \phi(m) \phi(n) \text{ for } \gcd(m,n) = 1. \)
  - \( \phi(pq) = (p-1)(q-1) \)

• Examples:
  - \( \phi(15) = \phi(3) \phi(5) = 2 \times 4 = 8. = \#\{1,2,4,7,8,11,13,14\} \)
  - \( \phi(9) = (3-1)3^{(2-1)} = 2 \times 3 = 6 = \#\{1,2,4,5,7,8\} \)
Euler’s Identity

• The number of elements in $\mathbb{Z}_n$ that have multiplicative inverses is equal to $\phi(n)$.

• Theorem: Let $(\mathbb{Z}_n)^*$ be the elements of $\mathbb{Z}_n$ with inverses (called units). If $a \in (\mathbb{Z}_n)^*$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. The same proof presented for Fermat’s theorem can be used to prove this theorem.
Chinese Remainder Theorem

Theorem: If \( \gcd(m,n) = 1 \), then given \( a \) and \( b \) there exist an integer solution to the system:
\[
x \equiv a \pmod{m} \text{ and } x = b \pmod{n}.
\]

Proof:
Consider the map \( x \mapsto (x \mod m, x \mod n) \).
This map is a 1-1 map from \( \mathbb{Z}_{mn} \) to \( \mathbb{Z}_m \times \mathbb{Z}_n \), since if \( x \) and \( y \) map to the same pair, then \( x \equiv y \pmod{m} \) and \( x \equiv y \pmod{n} \).
Since \( \gcd(m,n) = 1 \), this implies that \( x \equiv y \pmod{mn} \).
Since there are \( mn \) elements in both \( \mathbb{Z}_{mn} \) and \( \mathbb{Z}_m \times \mathbb{Z}_n \), the map is also onto. This means that for every pair \((a,b)\) we can find the desired \( x \).
**Alternative Interpretation of CRT**

- Let $Z_m \times Z_n$ denote the set of pairs $(a,b)$ where $a \in Z_m$ and $b \in Z_n$. We can perform arithmetic on $Z_m \times Z_n$ by performing componentwise modular arithmetic.
  
  - $(a,b) + (c,d) = (a+b, c+d)$
  - $(a,b)*(c,d) = (a*c, b*d)$

- **Theorem:** $Z_{mn} \approx Z_m \times Z_n$. I.E. There is a 1-1 mapping from $Z_{mn}$ onto $Z_m \times Z_n$ that preserves arithmetic.
  
  - $(a*c \mod m, b*d \mod n) = (a \mod m, b \mod n)*(c \mod m, d \mod n)$
  - $(a+c \mod m, b+d \mod n) = (a \mod m, b \mod n)+(c \mod m, d \mod n)$
  - The CRT implies that the map is onto. I.E. for every pair $(a,b)$ there is an integer $x$ such that $(x \mod m, x \mod n) = (a,b)$. 

Constructive Chinese Remainder Theorem

Theorem: If \( \gcd(m,n) = 1 \), then there exist \( e_m \) and \( e_n \) (orthogonal idempotents)

- \( e_m \equiv 1 \pmod{m} \)
- \( e_m \equiv 0 \pmod{n} \)
- \( e_n \equiv 0 \pmod{m} \)
- \( e_n \equiv 1 \pmod{n} \)

It follows that \( a^*e_m + b^*e_n \equiv a \pmod{m} \) and \( \equiv b \pmod{n} \).

Proof.

Since \( \gcd(m,n) = 1 \), by the Extended Euclidean Algorithm, there exist \( x \) and \( y \) with \( m^*x + n^*y = 1 \). Set \( e_m = n^*y \) and \( e_n = m^*x \).
Public Key Cryptosystem

Let M be a message and let C be the encrypted message (ciphertext). A public key cryptosystem has a separate method E() for encrypting and D() decrypting.

- \( D(E(M)) = M \)
- Both E() and D() are easy to compute
- Publicly revealing E() does not make it easy to determine D()
- \( E(D(M)) = M \) - needed for signatures

The collection of E()’s are made publicly available but the D()’s remain secret. Called a one-way trap-door function (hard to invert, but easy if you have the secret information)
RSA Public Key Cryptosystem

Based on the idea that it is hard to factor large numbers.

First encode M as an integer (e.g. use ASCII). Large messages will need to be blocked.

- Choose \( n = p \times q \), the product of two large prime numbers.
- Choose \( e \) such that \( \gcd(e, \phi(n)) = 1 \).
- Choose \( d \) such that \( de \equiv 1 \pmod{\phi(n)} \)

\[
\begin{align*}
E &= (e,n) \text{ and } E(M) = M^e \mod n \\
D &= (d,n) \text{ and } D(M) = M^d \mod n
\end{align*}
\]
Correctness of the RSA Algorithm

Theorem: \( D(E(M)) = E(D(M)) = M. \)

Proof. \( D(E(M)) = (M^e)^d \pmod{n} = M^{ed} \pmod{n}. \)
Since \( ed \equiv 1 \pmod{\varphi(n)} \), \( ed = k\varphi(n) + 1 \), for some integer \( k \).

\[
M^{k\varphi(n)+1} \rightarrow (M^{k\varphi(n)+1} \pmod{p}, M^{k\varphi(n)+1} \pmod{q})
\]
\[
= (M^{k\varphi(n)} \cdot M \pmod{p}, M^{k\varphi(n)} \cdot M \pmod{q})
\]
\[
= (M^{(p-1)(q-1)k} \cdot M \pmod{p}, M^{(q-1)(p-1)k} \cdot M \pmod{q}) \quad [\text{since } n = pq]
\]
\[
= ((M^{(p-1)})(q-1)k \cdot M \pmod{p}, (M^{(q-1)})(p-1)k \cdot M \pmod{q})
\]
\[
= (M \pmod{p}, M \pmod{q}) \quad [\text{By Fermat’s theorem}]
\]

Therefore, by the CRT, \( M^{k\varphi(n)+1} \equiv M \pmod{n}. \)