Number Theory and Group Theory for Public-Key Cryptography
TDA352, DIT250

Wissam Aoudi
Chalmers University of Technology

November 21, 2017
Textbook RSA Scheme

Key Generation:
- \textbf{KeyGen}(\lambda): pick two random \lambda-bit primes \( p, q \); set \( N = pq \); compute \( \varphi(N) \)
- choose an integer \( e \) in \( \mathbb{Z}_{\varphi(N)}^* \) and compute \( d = e^{-1} \pmod{\varphi(N)} \)
- output \( pk = (N, e) \) and \( sk = (N, d) \)

Encryption:
\[ \text{Enc}_{RSA}(pk, \cdot) : \mathbb{Z}_N^* \to \mathbb{Z}_N^* \text{ defined as } c = \text{Enc}_{RSA}(pk, m) = m^e \pmod{N} \]

Decryption:
\[ \text{Dec}_{RSA}(sk, \cdot) : \mathbb{Z}_N^* \to \mathbb{Z}_N^* \text{ defined as } m = \text{Dec}_{RSA}(sk, c) = c^d \pmod{N} \]

Correctness property
\[ \text{Dec}_{RSA}(sk, \text{Enc}_{RSA}(pk, m)) = \text{Dec}_{RSA}(sk, m^e) = m^{ed} = m^{k\varphi(N)+1} = m \pmod{N} \]
Outline

Textbook RSA Scheme

- **Key Generation:**
  - \(\text{KeyGen}(\lambda):\) pick two random \(\lambda\)-bit primes \(p, q\); set \(N = pq\); compute \(\varphi(N)\)
  - choose an integer \(e \in \mathbb{Z}_N^*\) and compute \(d = e^{-1} \pmod {\varphi(N)}\)
  - output \(pk = (N, e)\) and \(sk = (N, d)\)

- **Encryption:**
  - \(\text{Enc}_{RSA}(pk, \cdot) : \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*\) defined as \(c = \text{Enc}_{RSA}(pk, m) = m^e \pmod N\)

- **Decryption:**
  - \(\text{Dec}_{RSA}(sk, \cdot) : \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*\) defined as \(m = \text{Dec}_{RSA}(sk, c) = c^d \pmod N\)

- **Correctness property**
  - \(\text{Dec}_{RSA}(sk, \text{Enc}_{RSA}(pk, m)) = \text{Dec}_{RSA}(sk, m^e) = m^{ed} = m^{k\varphi(N)+1} = m \pmod N\)
Outline

Textbook RSA Scheme

- **Key Generation:**
  - **KeyGen(λ):** pick two random λ-bit primes \( p, q; \) set \( N = pq; \) compute \( \varphi(N) \)
  - choose an integer \( e \) in \( \mathbb{Z}_N^* \) and compute \( d = e^{-1} \pmod{\varphi(N)} \)
  - output \( pk = (N, e) \) and \( sk = (N, d) \)

- **Encryption:**
  \[ \text{Enc}_{RSA}(pk, \cdot) : \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^* \text{ defined as } c = \text{Enc}_{RSA}(pk, m) = m^e \pmod{N} \]

- **Decryption:**
  \[ \text{Dec}_{RSA}(sk, \cdot) : \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^* \text{ defined as } m = \text{Dec}_{RSA}(sk, c) = c^d \pmod{N} \]

- **Correctness property**
  \[ \text{Dec}_{RSA}(sk, \text{Enc}_{RSA}(pk, m)) = \text{Dec}_{RSA}(sk, m^e) = m^{ed} = m^{k\varphi(N)+1} = m \pmod{N} \]
Euclidean Division

Let \( a, b \in \mathbb{Z} \) with \( a > 0 \), then there exist unique integers \( q, r \) such that \( a = qb + r \), with \( 0 \leq r < b \).

Example

\[ a = 13, \ b = 6, \text{ then } 13 = 2 \times 6 + 1, \ (q = 2, \ r = 1) \]
**Definition (Prime Numbers)**

A positive integer $p > 1$ is said to be a **prime** if it is divisible by 1 and itself **only**.

**Example**

3, 5, 13, 19, 37, 83.

**Facts**

- Prime numbers are the *building blocks* of the natural numbers: any natural number $N > 1$ can be **uniquely** written as

  $$N = \prod_{i=1}^{n} p_{i}^{a_{i}} = p_{1}^{a_{1}} p_{2}^{a_{2}} \cdots p_{n}^{a_{n}}$$

  where $p_{1} < p_{2} < \cdots < p_{n}$ and $a_{i} \in \mathbb{N}$ (**Fundamental Theorem of Arithmetics**).

- Integer factorization is in general a **hard** problem.
**Greatest Common Divisor**

The **Greatest Common Divisor** of two integers is the largest integer that divides both of them.

**Definition (GCD)**

The **GCD** of two positive integers $a$ and $b$, is the positive integer $d$ such that

1. $d \mid a$ and $d \mid b$ (Common Divisor).
2. if $e \mid a$ and $e \mid b$, then $e \mid d$ (Greatest such divisor).

**Euclidean Algorithm**

```python
function gcd(a,b)
    if b = 0
        return a;
    else
        return gcd(b, a mod b);
```
Preliminaries: Extended Euclidean Algorithm (EEA)

Definition (Relative Primality)
If \( \text{GCD}(a, b) = 1 \), then \( a \) and \( b \) are said to be relatively prime (or coprime).

Definition (Bézout Identity)
Let \( a, b \) be two positive integers and \( d = \text{GCD}(a, b) \), then there exist integers \( s, t \in \mathbb{Z} \) such that \( d = as + bt \). In other words, \( d \) can be written as a linear combination of \( a, b \). One way to find a pair \( (s, t) \) is by using the Extended Euclidean Algorithm.

Example
Find the GCD of \( 456 \) and \( 100 \) and write it as a linear combination (using Extended Euclidean Algorithm)
### Extended Euclidean Algorithm (EEA)

<table>
<thead>
<tr>
<th>Remainder</th>
<th>456s + 100t</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>456</td>
<td>1 0</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>0 1</td>
<td></td>
</tr>
</tbody>
</table>
## Extended Euclidean Algorithm (EEA)

The Extended Euclidean Algorithm (EEA) is used to find the greatest common divisor (GCD) of two integers, as well as the coefficients of Bézout's identity, which are integers $s$ and $t$ such that:

$$ag + bh = 	ext{gcd}(a, b)$$

For example, let's find the GCD of 456 and 100 using the EEA:

\[
\begin{align*}
\text{Remainder} & \quad \text{456s} + \text{100t} \quad \text{Quotient} \\
456 & \quad 1 \quad 0 \\
100 & \quad 0 \quad 1 \\
\end{align*}
\]

\[
456 \div 100 = 4
\]

The GCD of 456 and 100 is 4, and the coefficients $s$ and $t$ are 1 and 0, respectively.
Extended Euclidean Algorithm (EEA)

<table>
<thead>
<tr>
<th>Remainder</th>
<th>456s + 100t</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>456</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>
### Extended Euclidean Algorithm (EEA)

<table>
<thead>
<tr>
<th>Remainder</th>
<th>456s + 100t</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>456</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>56</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

456 - 4*100 = 56
## Extended Euclidean Algorithm (EEA)

The Extended Euclidean Algorithm (EEA) is a method used to find the greatest common divisor (GCD) of two integers and, additionally, to find the coefficients such that the GCD is expressed as a linear combination of these two integers.

### Example

Given two numbers, 456 and 100, we can use the EEA to find the GCD and the coefficients such that:

\[ 456s + 100t = \gcd(456, 100) \]

<table>
<thead>
<tr>
<th>Remainder</th>
<th>456s + 100t</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>456</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>56</td>
<td>-</td>
<td>4</td>
</tr>
</tbody>
</table>

The GCD of 456 and 100 is 4, and the coefficients are s = 1 and t = 0.
Extended Euclidean Algorithm (EEA)

\[ 1 - 4 \times 0 = 1 \]

<table>
<thead>
<tr>
<th>Remainder</th>
<th>456s + 100t</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>456</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>56</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Extended Euclidean Algorithm (EEA)

<table>
<thead>
<tr>
<th>Remainder</th>
<th>456s + 100t</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>456</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>56</td>
<td>1</td>
<td>\cdot</td>
</tr>
</tbody>
</table>
Extended Euclidean Algorithm (EEA)

\[ 0 - 4 \times 1 = -4 \]

<table>
<thead>
<tr>
<th>Remainder</th>
<th>456s + 100t</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>456</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>56</td>
<td>1</td>
<td>-4</td>
</tr>
</tbody>
</table>
# Extended Euclidean Algorithm (EEA)

<table>
<thead>
<tr>
<th>Remainder</th>
<th>$456s + 100t$</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>456</td>
<td>1 0</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>0 1</td>
<td>4</td>
</tr>
<tr>
<td>56</td>
<td>1 -4</td>
<td></td>
</tr>
</tbody>
</table>
## Extended Euclidean Algorithm (EEA)

<table>
<thead>
<tr>
<th>Remainder</th>
<th>456s + 100t</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>456</td>
<td>1 0</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>0 1</td>
<td>4</td>
</tr>
<tr>
<td>56</td>
<td>1 -4</td>
<td>1</td>
</tr>
</tbody>
</table>

$100 \div 56 = 1$
## Extended Euclidean Algorithm (EEA)

### Table of Remainder, 456s, 100t, and Quotient

<table>
<thead>
<tr>
<th>Remainder</th>
<th>456s + 100t</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>456</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>56</td>
<td>1</td>
<td>-4</td>
</tr>
<tr>
<td>44</td>
<td>-1</td>
<td>5</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>-9</td>
</tr>
<tr>
<td>8</td>
<td>-7</td>
<td>32</td>
</tr>
<tr>
<td>4</td>
<td>9</td>
<td>-41</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Calculation

\[ 4 = 456 \times 9 - 100 \times 41 \]

### GCD and Bézout coefficients

- **GCD**: The final remainder, which is 0, indicates that the GCD of 456 and 100 is 4.
- **Bézout coefficients**: The coefficients 9 and -41 satisfy the equation \( 4 = 456 \times 9 - 100 \times 41 \).
### Modular Arithmetics

#### Definition (Congruence)

Let $a, b, n$ be positive integers such that $a, b$ have the same remainder upon dividing by $n$, then we say that $a$ is congruent to $b$ modulo $n$, written

$$a \equiv b \pmod{n}.$$ 

#### Facts

1. $a \equiv b \pmod{n} \Rightarrow n \mid a - b.$
2. $kn \equiv 0 \pmod{n}$ (for any $k \in \mathbb{Z}$).
3. $a \equiv b \pmod{n} \iff a = kn + b$ (for some $k \in \mathbb{Z}$).

#### Examples

- $23 \equiv 8 \pmod{5}$, since $23 = 3 \times 5 + 8$.
- $-1 \equiv 11 \pmod{6}$, since $6 \mid -1 - 11 = -12$.
- $7 \not\equiv 8 \pmod{3}$, since $3 \nmid 7 - 8 = -1$ (here $\mid$ means “does not divide”).
Modular Arithmetics

**Definition (Linear Congruence)**

A congruence of the form $ax \equiv b \pmod{n}$ is called a **linear congruence**, which has a solution if and only if there exists $x_0 \in \{0, 1, ..., n - 1\}$ such that $ax_0 \equiv b \pmod{n}$.

*Note that a linear congruence is like a linear equation except that it is solved modulo $n$.*

**Lemma**

The linear congruence $ax \equiv 1 \pmod{n}$ is **solvable** (i.e., has a solution) if and only if

$$\text{GCD}(a, n) = 1$$

(i.e., $a$ and $n$ are relatively prime).

**Very useful for computing modular inverses for RSA!**

Recall: in RSA we choose an encryption exponent $e$, and then compute the decryption exponent $d$ such that

$$d = e^{-1} \pmod{\varphi(N)} \iff e \cdot d \equiv 1 \pmod{\varphi(N)}.$$ 

That is, given $e$, we solve the **linear congruence** $e \cdot x \equiv 1 \pmod{\varphi(N)}$, the solution to which is exactly $d$, the “modular inverse” of $e$ in $\mathbb{Z}_{\varphi(N)}^*$. 
To find the **modular inverse** of an integer $a \pmod{n}$:

$$\gcd(a, n) = 1 \quad \text{(previous lemma)}$$

$$\Rightarrow ax + kn = 1 \quad \text{(Bézout lemma)}$$

$$\Rightarrow ax = 1 \pmod{n} \quad (kn = 0 \pmod{n})$$

$$\Rightarrow x = a^{-1} \pmod{n}.$$ 

We can find $x$ using EEA!

**Example**

Find the modular inverse of $2017 \pmod{397}$. 
<table>
<thead>
<tr>
<th>Remainder</th>
<th>X</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
Modular Arithmetics

\[ 2017 \div 397 = 5 \]

<table>
<thead>
<tr>
<th>Remainder</th>
<th>X</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>0</td>
<td>5</td>
</tr>
</tbody>
</table>
## Modular Arithmetics

<table>
<thead>
<tr>
<th>Remainder</th>
<th>X</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>0</td>
<td>5</td>
</tr>
</tbody>
</table>
### Modular Arithmetics

\[
2017 - 5 \times 397 = 32
\]

<table>
<thead>
<tr>
<th>Remainder</th>
<th>X</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>32</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Modular Arithmetics

<table>
<thead>
<tr>
<th>Remainder</th>
<th>$\times$</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>32</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Modular Arithmetics

1 - 5*0 = 1

<table>
<thead>
<tr>
<th>Remainder</th>
<th>X</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>32</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Remainder</td>
<td>X</td>
<td>Quotient</td>
</tr>
<tr>
<td>-----------</td>
<td>---</td>
<td>----------</td>
</tr>
<tr>
<td>2017</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>32</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
## Modular Arithmetics

<table>
<thead>
<tr>
<th>Remainder</th>
<th>X</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>32</td>
<td>1</td>
<td>12</td>
</tr>
</tbody>
</table>

$$397 \div 32 = 12$$
## Modular Arithmetics

<table>
<thead>
<tr>
<th>Remainder</th>
<th>X</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>32</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>13</td>
<td>-12</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>25</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>-62</td>
<td></td>
</tr>
</tbody>
</table>
### Modular Arithmetics

The given equation is: \( x = 2017^{-1} = -62 = 335 \pmod{397} \)

<table>
<thead>
<tr>
<th>Remainder</th>
<th>X</th>
<th>Quotient</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>32</td>
<td>-12</td>
<td>12</td>
</tr>
<tr>
<td>13</td>
<td>25</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>-62</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**GCD**

**Modular inverse**
Textbook RSA Scheme

**Key Generation:**
- \( \text{KeyGen}(\lambda) \): pick two random \( \lambda \)-bit primes \( p, q \); set \( N = pq \); compute \( \varphi(N) \)
- choose an integer \( e \) in \( \mathbb{Z}_\varphi^*(N) \) and compute \( d = e^{-1} \pmod{\varphi(N)} \)
- output \( pk = (N, e) \) and \( sk = (N, d) \)

**Encryption:**
\[
\text{Enc}_{\text{RSA}}(pk, \cdot) : \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^* \text{ defined as } c = \text{Enc}_{\text{RSA}}(pk, m) = m^e \pmod{N}
\]

**Decryption:**
\[
\text{Dec}_{\text{RSA}}(sk, \cdot) : \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^* \text{ defined as } m = \text{Dec}_{\text{RSA}}(sk, c) = c^d \pmod{N}
\]

**Correctness property**
\[
\text{Dec}_{\text{RSA}}(sk, \text{Enc}_{\text{RSA}}(pk, m)) = \text{Dec}_{\text{RSA}}(sk, m^e) = m^{ed} = m^{k\varphi(N)+1} = m \pmod{N}
\]
Euler’s Totient Function

**Definition (Totient Function)**

The **totient function** (or **Euler Phi function**) \( \varphi(\cdot) : \mathbb{N} \to \mathbb{N} \), is defined to be the number of positive integers less than \( n \) and relatively prime to \( n \). That is,

\[
\varphi(n) = |\{k \in \mathbb{N}, \text{ such that } k < n \text{ and } \text{GCD}(n, k) = 1 \}|.
\]

**Facts (important for RSA!)**

- If \( p \) is prime, then \( \varphi(p) = p - 1 \).
- If \( N = pq \), where \( p, q \) are primes, then \( \varphi(N) = (p - 1)(q - 1) \). Why?
  - \( \varphi \) is a **multiplicative** function, meaning that, if \( \text{GCD}(a, b) = 1 \), then \( \varphi(ab) = \varphi(a)\varphi(b) \).
  - As \( p, q \) are primes, \( \varphi(p) = p - 1 \) and \( \varphi(q) = q - 1 \).
Euler’s Totient Function

Example

- \( \varphi(10) = |\{1, 3, 7, 9\}| = 4. \)
- \( \varphi(7) = |\{1, 2, 3, 4, 5, 6\}| = 6. \) Is there a formula for \( \varphi(N) \)? Yes!

Formula for \( \varphi(N) \)

We have

- \( \varphi(p^a) = p^{a-1}(p - 1) \).
- \( \varphi \) is multiplicative, hence \( \varphi(ab) = \varphi(a)\varphi(b) \).
- \( N = p_1^{a_1}p_2^{a_2} \cdots p_n^{a_n} \)

Thus

\[
\varphi(N) = \varphi(p_1^{a_1}p_2^{a_2} \cdots p_n^{a_n}) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdots \varphi(p_n^{a_n}) \\
= p_1^{a_1-1}(p_1 - 1)p_2^{a_2-1}(p_2 - 1) \cdots p_n^{a_n-1}(p_n - 1).
\]

Example

\[
\varphi(600) = \varphi(2^3 \cdot 3 \cdot 5^2) = \varphi(2^3) \cdot \varphi(3) \cdot \varphi(5^2) = 2^2(2 - 1) \cdot (3 - 1) \cdot 5(5 - 1) = 160.
\]

Note that to compute \( \varphi(N) \), we need to know the prime decomposition of \( N \). Good news for RSA! Finding \( \varphi(N) \) (without knowing \( p \) or \( q \)) is as hard as factoring \( N \).
Key Generation:
- \( \text{KeyGen}(\lambda) \): pick two random \( \lambda \)-bit primes \( p, q \); set \( N = pq \); compute \( \varphi(N) \)
- choose an integer \( e \) in \( \mathbb{Z}_N^* \) and compute \( d = e^{-1} \pmod{\varphi(N)} \)
- output \( pk = (N, e) \) and \( sk = (N, d) \)

Encryption:
\( \text{Enc}_{\text{RSA}}(pk, \cdot) : \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^* \) defined as \( c = \text{Enc}_{\text{RSA}}(pk, m) = m^e \pmod{N} \)

Decryption:
\( \text{Dec}_{\text{RSA}}(sk, \cdot) : \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^* \) defined as \( m = \text{Dec}_{\text{RSA}}(sk, c) = c^d \pmod{N} \)

Correctness property
\( \text{Dec}_{\text{RSA}}(sk, \text{Enc}_{\text{RSA}}(pk, m)) = \text{Dec}_{\text{RSA}}(sk, m^e) = m^{ed} = m^{\varphi(N)+1} = m \pmod{N} \)
Fermat’s Theorem & Euler’s Theorem

Fermat’s Theorem
Let \( a \) be a positive integer, and \( p \) a prime such that \( p \) does not divide \( a \), then
\[
a^{p-1} \equiv 1 \pmod{p}.
\]

Example
\[
5^{38} \equiv ? \pmod{13}.
\]
\[
a = 5, \ p = 13 \quad \text{(note that } \ 13 \nmid 5),
\]
\[
5^{38} \equiv (5^{12})^3 \cdot 5^2 \equiv (1)^3 \cdot 25 \equiv 1 \cdot 12 \equiv 12 \pmod{13}.
\]

Euler’s Theorem
Let \( a, n \) be two relatively prime positive integers with \( n > 1 \), then
\[
a^{\phi(n)} \equiv 1 \pmod{n}.
\]

Exercise: Find the remainder of \( 3^{35} \) when divided by \( 20 \).
Correctness Property

Why $m^{ed} = m \pmod{N}$?

\[
d = e^{-1} \pmod{\varphi(N)}
\]
\[
\Rightarrow e \cdot d = 1 \pmod{\varphi(N)}
\]
\[
\Rightarrow e \cdot d = k\varphi(N) + 1
\]

\[
m^{ed} \pmod{N} = m^{k\varphi(N)+1} \pmod{N}
\]
\[
= m^{k\varphi(N)} \cdot m \pmod{N}
\]
\[
= (m^{\varphi(N)})^k \cdot m \pmod{N}
\]
\[
= (1)^k \cdot m \pmod{N}
\]
\[
= m \pmod{N}
\]
Outline

Textbook RSA Scheme

- **Key Generation:**
  - \( \text{KeyGen}(\lambda) \): pick two random \( \lambda \)-bit primes \( p, q \); set \( N = pq \); compute \( \varphi(N) \)
  - choose an integer \( e \) in \( \mathbb{Z}_N^* \) and compute \( d = e^{-1} \pmod{\varphi(N)} \)
  - output \( pk = (N, e) \) and \( sk = (N, d) \)

- **Encipherment:**
  - \( \text{Enc}_{RSA}(pk, \cdot) : \mathbb{Z}_N^* \to \mathbb{Z}_N^* \) defined as \( c = \text{Enc}_{RSA}(pk, m) = m^e \pmod{N} \)

- **Decipherment:**
  - \( \text{Dec}_{RSA}(sk, \cdot) : \mathbb{Z}_N^* \to \mathbb{Z}_N^* \) defined as \( m = \text{Dec}_{RSA}(sk, c) = c^d \pmod{N} \)

- **Correctness property**
  - \( \text{Dec}_{RSA}(sk, \text{Enc}_{RSA}(pk, m)) = \text{Dec}_{RSA}(sk, m^e) = m^{ed} = m^{k\varphi(N)+1} = m \pmod{N} \)
Chinese Remainder Theorem (a special case)

Let $N = pq$, where $p, q$ are distinct primes, and let $a, b$ be any two integers, then the system of linear congruences

$$\begin{align*}
    x &\equiv a \pmod{p} \\
    x &\equiv b \pmod{q}
\end{align*}$$

is solvable, and has a unique solution modulo $pq$. Moreover, the unique solution $x$ is given by $x = atq + bsp$, where $s, t$ are the Bézout coefficients of $p, q$ respectively (i.e., $s, t$ satisfy $sp + tq = 1$).

Motivation

The importance of **CRT** is that if the prime factors $p, q$ of an integer $N$ are known, then computations modulo $N$ can be reduced to computations modulo $p$ and $q$ separately. In RSA, $p, q$ are chosen to be of roughly the same size ($\sim \sqrt{N}$), and for a sufficiently large value of $N$, $\sqrt{N}$ is much smaller than $N$, and consequently arithmetics modulo $p$ and $q$ are much cheaper to perform.
Textbook RSA Scheme

**Key Generation:**
- \(\text{KeyGen}(\lambda)\): pick two random \(\lambda\)-bit primes \(p, q\); set \(N=pq\); compute \(\varphi(N)\)
- choose an integer \(e\) in \(\mathbb{Z}^*_\varphi(N)\) and compute \(d = e^{-1} \pmod{\varphi(N)}\)
- output \(pk = (N, e)\) and \(sk = (N, d)\)

**Encryption:**
\[\text{Enc}_{RSA}(pk, \cdot) : \mathbb{Z}^*_N \rightarrow \mathbb{Z}^*_N\] defined as \(c = \text{Enc}_{RSA}(pk, m) = m^e \pmod{N}\)

**Decryption:**
\[\text{Dec}_{RSA}(sk, \cdot) : \mathbb{Z}^*_N \rightarrow \mathbb{Z}^*_N\] defined as \(m = \text{Dec}_{RSA}(sk, c) = c^d \pmod{N}\)

**Correctness property**
\[\text{Dec}_{RSA}(sk, \text{Enc}_{RSA}(pk, m)) = \text{Dec}_{RSA}(sk, m^e) = m^{ed} = m^{k\varphi(N)+1} = m \pmod{N}\]
Consider the group of all integers \( \mathbb{Z} = \{ \cdots, -2, -1, 0, 1, 2, \cdots \} \).

- For all \( a, b \in \mathbb{Z} \), \( a + b \in \mathbb{Z} \) (we say \( \mathbb{Z} \) is closed under addition).
- For all \( a, b, c \in \mathbb{Z} \), \( (a + b) + c = a + (b + c) \) (\( \mathbb{Z} \) is associative).
- For every element \( a \in \mathbb{Z} \), \( a + 0 = 0 + a = a \) (0 is the identity in \( \mathbb{Z} \)).
- For every element \( a \in \mathbb{Z} \), there exists an element \( b = -a \in \mathbb{Z} \), such that \( a + b = b + a = 0 \) (every element in \( \mathbb{Z} \) has an additive inverse).

We say that \( \mathbb{Z} \) is a **Group Under Addition**.
**Definition (Group Under Addition)**

A group $G$ is a set, together with an operation $+$, satisfying the following properties

1. **Closure** For all $a, b \in G$, the result of the operation $+$, i.e., $a + b$, is also in $G$.
2. **Associativity** For all $a, b, c \in G$, it holds that, $(a + b) + c = a + (b + c)$.
3. **Identity Element** There exists an element $e \in G$, such that, for every element $a \in G$, it holds that $a + e = e + a = a$.
4. **Inverse Element** For each $a \in G$, there exists an element $b \in G$, such that $a + b = b + a = e$ (the inverse of $a$ is usually denoted as $-a$).

**Definition (Group Under Multiplication)**

A group $G$ is a set, together with an operation $\cdot$, satisfying the following properties

1. **Closure** For all $a, b \in G$, the result of the operation $\cdot$, i.e., $a \cdot b$, is also in $G$.
2. **Associativity** For all $a, b, c \in G$, it holds that, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. **Identity Element** There exists an element $e \in G$, such that, for every element $a \in G$, it holds that $a \cdot e = e \cdot a = a$.
4. **Inverse Element** For each $a \in G$, there exists an element $b \in G$, such that $a \cdot b = b \cdot a = e$ (the inverse of $a$ is usually denoted as $a^{-1}$).
We showed that \( \mathbb{Z} \) is a group under addition.

But \( \mathbb{Z} \) is not a group under multiplication, because although closed, associative, and has identity 1, there exists an element (in fact all elements except for 1 and \(-1\)) that has no inverse. For instance, 5 is in \( \mathbb{Z} \), but \( 5 \cdot x = 1 \) has no solution in \( \mathbb{Z} \).

On the other hand, the set of rational numbers \( \mathbb{Q} \) (without the element 0), is a group under multiplication, since it is closed, associative, has identity 1, and for every element \( a \in \mathbb{Q} \), the linear equation \( a \cdot x = 1 \) always has the solution \( x = a^{-1} = 1/a \) (in particular, \( 5^{-1} = 1/5 \)).
Group of Integers Modulo N

Define $\mathbb{Z}_N$ as the set of integers modulo $N$ (e.g., $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$), then $\mathbb{Z}_N$ is a group under addition. Let us prove this for $N = 3$, i.e., for $\mathbb{Z}_3 = \{0, 1, 2\}$.

1. **Closure**

\[
\begin{align*}
0 + 0 &= 0 \pmod{3} & 0 + 2 &= 2 \pmod{3} & 1 + 2 &= 3 = 0 \pmod{3} \\
0 + 1 &= 1 \pmod{3} & 1 + 1 &= 2 \pmod{3} & 2 + 2 &= 4 = 1 \pmod{3}
\end{align*}
\]

2. **Associativity**

\[
(0 + 1) + 2 = 0 + (1 + 2) \pmod{3}
\]

3. **Identity Element**

\[
\begin{align*}
0 + 0 &= 0 \pmod{3} & 1 + 0 &= 1 \pmod{3} & 2 + 0 &= 2 \pmod{3}
\end{align*}
\]

4. **Inverses**

\[
\begin{align*}
0 + 0 &= 0 \pmod{3} & 1 + (-1) &= 1 + 2 = 3 = 0 \pmod{3} & 2 + (-2) &= 2 + 1 = 3 = 0 \pmod{3}
\end{align*}
\]

But $\mathbb{Z}_6$ is not a group under multiplication because not every element has an inverse (e.g., there exists no $x \in \mathbb{Z}_6$ such that $4 \cdot x = 1 \pmod{6}$).
Group Theory

So, to make the set of integers modulo \( N \) a group under multiplication, we should only choose the elements \( a \) that have inverses, i.e., for which there exists \( x \) such that \( a \cdot x \equiv 1 \pmod{N} \).

Recall the lemma: \( a \cdot x \equiv 1 \pmod{N} \) if and only if \( \text{GCD}(a, N) = 1 \).

### Multiplicative Group of Integers Modulo \( N \)

Define \( \mathbb{Z}_N^* \) to be the set of integers \textit{modulo} \( N \) and \textit{relatively prime to} \( N \), that is,

\[ \mathbb{Z}_N^* = \{ a \in \mathbb{Z}_N, \text{ such that } \text{GCD}(a, N) = 1 \}. \]

Then, \( \mathbb{Z}_N^* \) is a \textit{group under multiplication}.

### Example

- \( \mathbb{Z}_6^* = \{ 1, 5 \} \).
- \( \mathbb{Z}_{14}^* = \{ 1, 3, 5, 9, 11, 13 \} \).
- \( \mathbb{Z}_{11}^* = \{ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \} \).

\( \mathbb{Z}_N^* \) is a fundamental group for RSA! It is an \textit{algebraic structure} where the \textit{correctness property} of RSA holds.
Group Theory

Definition (Order of a Group)

The order of a group $G$ is its cardinality, i.e., the number of elements in its set. It is denoted as $\text{ord}(G)$ or $|G|$.

Example

- $\text{ord}(\mathbb{Z}_4) = |\{0, 1, 2, 3\}| = 4$
- $\text{ord}(\mathbb{Z}_N) = |\{0, 1, \ldots, N-1\}| = N$
- $\text{ord}(\mathbb{Z}_N^*)$ = ?

Lemma

The order of $\mathbb{Z}_N^*$ is $\varphi(N)$. [recall the definition of $\varphi(N)$]

Example

$|\mathbb{Z}_{15}^*| = \varphi(15) = \varphi(3 \cdot 5) = (3 - 1)(5 - 1) = 8. \quad [\text{recall that } \varphi(p \cdot q) = (p - 1)(q - 1) \text{ if } p, q \text{ are primes}]$
Definition (Order of an Element in a Group)

The order of an element \(a\) in a (multiplicative) group \(G\) is the smallest positive integer \(n\) such that \(a^n = e\), where \(e\) is the (multiplicative) identity element of \(G\).

Example

\[\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}\]  \(\text{[note: In } \mathbb{Z}_N^*, \text{ the identity is always } 1]\)

What is the order of 2 in \(\mathbb{Z}_9^*\)?

\[
\begin{align*}
2^1 &= 2 \neq 1 \text{ in } \mathbb{Z}_9^* \\
2^2 &= 4 \neq 1 \text{ in } \mathbb{Z}_9^* \\
2^3 &= 8 \neq 1 \text{ in } \mathbb{Z}_9^* \\
2^4 &= 16 = 7 \neq 1 \text{ in } \mathbb{Z}_9^* \\
2^5 &= 32 = 5 \neq 1 \text{ in } \mathbb{Z}_9^* \\
2^6 &= 64 = 1 \text{ in } \mathbb{Z}_9^* 
\end{align*}
\]

Note: \(\text{ord}(2) = \text{ord}(\mathbb{Z}_9^*) \Rightarrow 2\) is a generator of \(\mathbb{Z}_9^*\), which means that \(\mathbb{Z}_9^*\) is a cyclic group (definition in a couple of slides).
For every element \( a \) of a group \( G \), it holds that the order of \( a \) divides the order of \( G \), i.e.,

\[
\text{ord}(a) \mid \text{ord}(G).
\]

Example

\( \mathbb{Z}^*_9 = \{1, 2, 4, 5, 7, 8\} \), \( |\mathbb{Z}^*_9| = \varphi(9) = 6 \)

What is the order of 2 in \( \mathbb{Z}^*_9 \)?

\[
\begin{align*}
2^1 &= 2 \neq 1 \text{ in } \mathbb{Z}^*_9 \\
2^2 &= 4 \neq 1 \text{ in } \mathbb{Z}^*_9 \\
2^3 &= 8 \neq 1 \text{ in } \mathbb{Z}^*_9 \\
2^4 &= 16 = 7 \neq 1 \text{ in } \mathbb{Z}^*_9 \\
2^5 &= 32 = 5 \neq 1 \text{ in } \mathbb{Z}^*_9 \\
2^6 &= 64 = 1 \text{ in } \mathbb{Z}^*_9
\end{align*}
\]

since \( |2| \) in \( \mathbb{Z}^*_9 \) must be a divisor of 6, i.e., 1, 2, 3, or 6. This means that we do not need to check \( 2^4, 2^5 \) since 4, 5 are not divisors of 6.
Definition (Subgroups)

A non-empty subset $H$ of a group $G$ is said to be a subgroup of $G$, if $H$ is itself a group under the same operation of $G$.

Definition (Subgroup generated by an element)

Let $G$ be a group and $a \in G$. Define

$$< a > = \{ a^i, \ i \in \mathbb{N} \}$$

then, $< a >$ is a subgroup of $G$, called the subgroup generated by $a$.

Lemma (Group Generator)

An element $a$ of a group $G$ is called a generator of $G$ if $< a > = G$. That is, every element $g$ of $G$ can be written as a power of $a$, i.e.,

for all $g \in G$, $g = a^k$ ($k \in \mathbb{N}$).
Definition (Cyclic Groups)

A group $G$ is said to be a **cyclic group** if it has a group generator, i.e., if there exists an element $a \in G$ such that $\langle a \rangle = G$.

Moreover, $a$ is a generator of $G$ if and only if $|\langle a \rangle| = |a| = |G|$.

**Example**

In $\mathbb{Z}^*_{11}$, 2 is a generator since: [recall first that $|2|$ divides $|\mathbb{Z}^*_{11}|$]

we have $|\mathbb{Z}^*_{11}| = \varphi(11) = 10$, and in $\mathbb{Z}^*_{11}$

$$2^1 = 2 \neq 1$$

$$2^2 = 4 \neq 1$$

$$2^5 = 32 = 10 \neq 1$$

$$2^{10} = 1024 = 1$$

Thus, $|2| = 10 = |\mathbb{Z}^*_{11}|$. Therefore 2 is a **generator** of $\mathbb{Z}^*_{11}$ and $\mathbb{Z}^*_{11}$ is cyclic.

Indeed $\mathbb{Z}^*_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = \{2^0, 2^1, 2^8, 2^2, 2^4, 2^9, 2^7, 2^3, 2^6, 2^5\}$.

**Exercise:** Show that $\mathbb{Z}^*_8$ is not cyclic and list all its subgroups.

In fact, $\mathbb{Z}^*_N$ is cyclic if and only if $N = 2, 4, p^a, 2p^a$ ($p > 2$ a prime, $a \in \mathbb{N}$).
Lemma

Let $G$ be a group with identity element $e$, and let $a \in G$, then

$$a|G| = e.$$ 

Revisiting Euler’s and Fermat’s Theorems

Let $a \in \mathbb{Z}_N^*$, then
- $a$ is relatively prime to $N$, i.e., $\text{GCD}(a, N) = 1$.
- $|\mathbb{Z}_N^*| = \varphi(N)$.

Therefore by the previous lemma, $a|\mathbb{Z}_N^*| = a^{\varphi(N)} = 1$ in $\mathbb{Z}_N^*$, or equivalently

$$a^{\varphi(N)} \equiv 1 \pmod{N}. \quad [\text{Euler’s Theorem!}]$$

Fermat’s theorem is a special case where $a \in \mathbb{Z}_p^*$, where $p$ is prime, so that

$$a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod{p}.$$
References

2. “Introduction to Modern Cryptography”, Lindell and Katz (Chapter 7.1.1, 7.1.3, 7.1.4, 7.2).”

Thank you for your attention!