Number Theory, Public-Key Cryptography, and the RSA Cryptosystem

Douglas Wikström
KTH Stockholm
dog@csc.kth.se

February 4

- Number Theory
- Public-Key Cryptography
- The RSA Cryptosystem

Quote of the Day

The Magic Words are Squeamish Ossifrage

– Rivest's RSA-129 challenge plaintext from 1977.

(broken in 1994)

Greatest Common Divisors

Definition. A common divisor of two integers m and n is an integer d such that $d \mid m$ and $d \mid n$.

Definition. A greatest common divisor (GCD) of two integers m and n is a common divisor d such that every common divisor d' divides d.

Greatest Common Divisors

Definition. A common divisor of two integers m and n is an integer d such that $d \mid m$ and $d \mid n$.

Definition. A greatest common divisor (GCD) of two integers m and n is a common divisor d such that every common divisor d' divides d.

- **The** GCD is the **positive** GCD.

Greatest Common Divisors

Definition. A common divisor of two integers m and n is an integer d such that $d \mid m$ and $d \mid n$.

Definition. A greatest common divisor (GCD) of two integers m and n is a common divisor d such that every common divisor d' divides d.

- **The** GCD is the **positive** GCD.
- We denote the GCD of m and n by $\gcd(m, n)$.

Properties

- $\gcd(m, n) = \gcd(n, m)$
- $\gcd(m, n) = \gcd(m \pm n, n)$
- $\gcd(m, n) = \gcd(m \bmod n, n)$
- $\gcd(m, n) = 2\gcd(m/2, n/2)$ if m and n are even.
- $\gcd(m, n) = \gcd(m/2, n)$ if m is even and n is odd.

Euclidean Algorithm

EUCLIDEAN(m, n)
(1) **while** $n \neq 0$
(2) $t \leftarrow n$
(3) $n \leftarrow m \bmod n$
(4) $m \leftarrow t$
(5) **return** m

Steins Algorithm (Binary GCD Algorithm)

```
STEIN(m, n)
    if m = 0 or n = 0 then return 0
    s ← 0
    while m and n are even
        m ← m/2, n ← n/2, s ← s + 1
    while n is even
        n ← n/2
    while m ≠ 0
        while m is even
            m ← m/2
        if m < n
            SWAP(m, n)
        m ← m − n
        m ← m/2
    return 2^s m
```

Bezout's Lemma

Lemma. There exists integers a and b such that

$$\gcd(m, n) = am + bn \quad .$$

Bezout's Lemma

Lemma. There exists integers a and b such that

$$\gcd(m, n) = am + bn \ .$$

Proof. Let $d > \gcd(m, n)$ be the smallest positive integer on the form $d = am + bn$. Write $m = cd + r$ with $0 \leq r < d$. Then

$$d > r = m - cd = m - c(am + bn) = (1 - ca)m + (-cb)n \ ,$$

a contradiction! Thus, $r = 0$ and $d \mid m$. Similarly, $d \mid n$.

Bezout's Lemma

Lemma. There exists integers a and b such that

$$\gcd(m, n) = am + bn \ .$$

Proof. Let $d > \gcd(m, n)$ be the smallest positive integer on the form $d = am + bn$. Write $m = cd + r$ with $0 \leq r < d$. Then

$$d > r = m - cd = m - c(am + bn) = (1 - ca)m + (-cb)n \ ,$$

a contradiction! Thus, $r = 0$ and $d \mid m$. Similarly, $d \mid n$.

Why is d the **greatest** common divisor?

Extended Euclidean Algorithm (Recursive Version)

$\textsc{ExtendedEuclidean}(m,\ n)$
(1) **if** $m \bmod n = 0$
(2) **return** $(0, 1)$
(3) **else**
(4) $(x, y) \leftarrow \textsc{ExtendedEuclidean}(n, m \bmod n)$
(5) **return** $(y, x - y\lfloor m/n \rfloor)$

If $(x, y) \leftarrow \textsc{ExtendedEuclidean}(m, n)$ then
$\gcd(m, n) = xm + yn$.

Coprimality (Relative Primality)

Definition. Two integers m and n are coprime if their greatest common divisor is ± 1.

Fact. If a and n are coprime, then there exists a b such that $ab = 1 \bmod n$.

Coprimality (Relative Primality)

Definition. Two integers m and n are coprime if their greatest common divisor is ± 1.

Fact. If a and n are coprime, then there exists a b such that $ab = 1 \bmod n$.

Excercise: Why is this so?

Chinese Remainder Theorem (CRT)

Theorem. (Sun Tzu 400 AC) Let $n_1, \ldots, n_k$ be positive pairwise coprime integers and let $a_1, \ldots, a_k$ be integers. Then the equation system

$$\begin{array}{rcl} x & = & a_1 \bmod n_1 \\ x & = & a_2 \bmod n_2 \\ x & = & a_3 \bmod n_3 \\ & \vdots & \\ x & = & a_k \bmod n_k \end{array}$$

has a unique solution in $\{0, \ldots, \prod_i n_i - 1\}$.

Constructive Proof of CRT

1. Set $N = n_1 n_2 \cdot \ldots \cdot n_k$.
2. Find r_i and s_i such that $r_i n_i + s_i \frac{N}{n_i} = 1$ (Bezout).
3. Note that

$$s_i \frac{N}{n_i} = 1 - r_i n_i = \begin{cases} 1 \pmod{n_i} & \\ 0 \pmod{n_j} & \text{if } j \neq i \end{cases}$$

4. The solution to the equation system becomes:

$$x = \sum_{i=1}^{k} \left(s_i \frac{N}{n_i} \right) \cdot a_i$$

The Multiplicative Group

The set $\mathbb{Z}_n^* = \{0 \leq a < n \ : \ \gcd(a, n) = 1\}$ forms a group, since:

- **Closure.** It is closed under multiplication modulo n.
- **Associativity.** For $x, y, z \in \mathbb{Z}_n^*$:
$$(xy)z = x(yz) \bmod n \ .$$
- **Identity.** For every $x \in \mathbb{Z}_n^*$:
$$1 \cdot x = x \cdot 1 = x \ .$$
- **Inverse.** For every $a \in \mathbb{Z}_n^*$ exists $b \in \mathbb{Z}_n^*$ such that:
$$ab = 1 \bmod n \ .$$

Lagrange's Theorem

Theorem. If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Proof.

1. Define $aH = \{ah : h \in H\}$. This gives an equivalence relation $x \approx y \Leftrightarrow x = yh \wedge h \in H$ on G.
2. The map $\phi_{a,b} : aH \to bH$, defined by $\phi_{a,b}(x) = ba^{-1}x$ is a bijection, so $|aH| = |bH|$ for $a, b \in G$.

Euler's Phi-Function (Totient Function)

Definition. Euler's Phi-function $\phi(n)$ counts the number of integers $0 < a < n$ relative prime to n.

Euler's Phi-Function (Totient Function)

Definition. Euler's Phi-function $\phi(n)$ counts the number of integers $0 < a < n$ relative prime to n.

- Clearly: $\phi(p) = p - 1$ when p is prime.

Euler's Phi-Function (Totient Function)

Definition. Euler's Phi-function $\phi(n)$ counts the number of integers $0 < a < n$ relative prime to n.

- Clearly: $\phi(p) = p - 1$ when p is prime.
- Similarly: $\phi(p^k) = p^k - p^{k-1}$ when p is prime and $k > 1$.

Euler's Phi-Function (Totient Function)

Definition. Euler's Phi-function $\phi(n)$ counts the number of integers $0 < a < n$ relative prime to n.

- Clearly: $\phi(p) = p - 1$ when p is prime.
- Similarly: $\phi(p^k) = p^k - p^{k-1}$ when p is prime and $k > 1$.
- In general: $\phi\left(\prod_i p_i^{k_i}\right) = \prod_i \left(p_i^k - p_i^{k-1}\right)$.

Euler's Phi-Function (Totient Function)

Definition. Euler's Phi-function $\phi(n)$ counts the number of integers $0 < a < n$ relative prime to n.

- Clearly: $\phi(p) = p - 1$ when p is prime.
- Similarly: $\phi(p^k) = p^k - p^{k-1}$ when p is prime and $k > 1$.
- In general: $\phi\left(\prod_i p_i^{k_i}\right) = \prod_i \left(p_i^k - p_i^{k-1}\right)$.

  Excercise: How does this follow from CRT?

Fermat's and Euler's Theorems

Theorem. (Fermat) If $b \in \mathbb{Z}_p^*$ and p is prime, then $b^{p-1} = 1 \bmod p$.

Theorem. (Euler) If $b \in \mathbb{Z}_n^*$, then $b^{\phi(n)} = 1 \bmod n$.

Fermat's and Euler's Theorems

Theorem. (Fermat) If $b \in \mathbb{Z}_p^*$ and p is prime, then $b^{p-1} = 1 \bmod p$.

Theorem. (Euler) If $b \in \mathbb{Z}_n^*$, then $b^{\phi(n)} = 1 \bmod n$.

Proof. Note that $|\mathbb{Z}_n^*| = \phi(n)$. b generates a subgroup $\langle b \rangle$ of $\mathbb{Z}_n^*$, so $|\langle b \rangle|$ divides $\phi(n)$ and $b^{\phi(n)} = 1 \bmod n$.

Fermat's and Euler's Theorems

Theorem. (Fermat) If $b \in \mathbb{Z}_p^*$ and p is prime, then $b^{p-1} = 1 \bmod p$.

Theorem. (Euler) If $b \in \mathbb{Z}_n^*$, then $b^{\phi(n)} = 1 \bmod n$.

Proof. Note that $|\mathbb{Z}_n^*| = \phi(n)$. b generates a subgroup $\langle b \rangle$ of $\mathbb{Z}_n^*$, so $|\langle b \rangle|$ divides $\phi(n)$ and $b^{\phi(n)} = 1 \bmod n$.

Excercise: What happens when $b \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$?

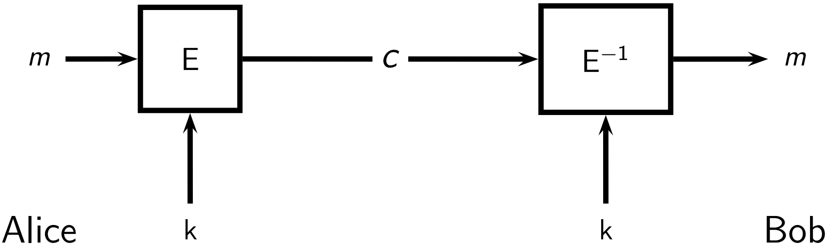
Multiplicative Group of a Prime Order Field

Definition. A group G is called **cyclic** if there exists an element g such that each element in G is on the form g^x for some integer x.

Theorem. If p is prime, then $\mathbb{Z}_p^*$ is cyclic.

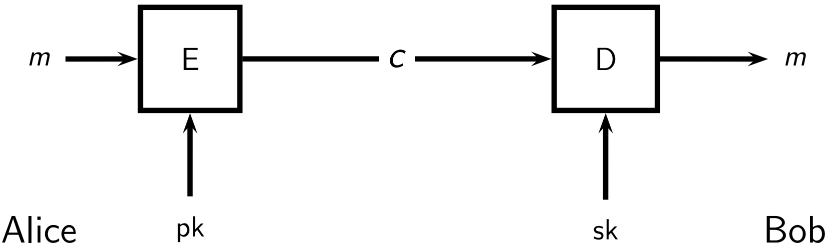
Cipher (Symmetric Cryptosystem)

$$c = \mathsf{E}_{\mathsf{k}}(m) \qquad\qquad m = \mathsf{E}_{\mathsf{k}}^{-1}(c)$$



Public-Key Cryptosystem

$c = \mathsf{E}_{\mathsf{pk}}(m)$ $m = \mathsf{D}_{\mathsf{sk}}(c)$



History of Public-Key Cryptography

Public-key cryptography was discovered:

- By Ellis, Cocks, and Williamson at the Government Communications Headquarters (GCHQ) in the UK in the early 1970s (not public until 1997).
- Independently by Merkle in 1974 (Merkle's puzzles).
- Independently in its discrete-logarithm based form by Diffie and Hellman in 1977, and instantiated in 1978 (key-exchange).
- Independently in its factoring-based form by Rivest, Shamir and Adleman in 1977.

Public-Key Cryptography

Definition. A public-key cryptosystem is a tuple $(\mathsf{Gen}, \mathsf{E}, \mathsf{D})$ where,

- Gen is a **probabilistic key generation algorithm** that outputs key pairs $(\mathsf{pk}, \mathsf{sk})$,
- E is a (possibly probabilistic) **encryption algorithm** that given a public key pk and a message m in the plaintext space $\mathcal{M}_{\mathsf{pk}}$ outputs a ciphertext c, and
- D is a decryption algorithm that given a secret key sk and a ciphertext c outputs a plaintext m,

such that $\mathsf{D}_{\mathsf{sk}}(\mathsf{E}_{\mathsf{pk}}(m)) = m$ for every public-key pk and $m \in \mathcal{M}_{\mathsf{pk}}$.

The RSA Cryptosystem (1/2)

Key Generation.

- Choose n-bit primes p and q randomly and define $N = pq$.
- Choose e randomly in $\mathbb{Z}^*_{\phi(N)}$ and compute $d = e^{-1} \bmod \phi(N)$.
- Output the key pair $((N, e), (p, q, d))$, where (N, e) is the public key and (p, q, d) is the secret key.

The RSA Cryptosystem (2/2)

Encryption. Encrypt a plaintext m by computing

$$c = m^e \bmod N \enspace .$$

Decryption. Decrypt a ciphertext c by computing

$$m = c^d \bmod N \enspace .$$

Why Does It Work?

$$(m^e \bmod N)^d \bmod N = m^{ed} \bmod N$$

Why Does It Work?

$$
\begin{aligned}
(m^e \bmod N)^d \bmod N &= m^{ed} \bmod N \\
&= m^{1+t\phi(N)} \bmod N
\end{aligned}
$$

Why Does It Work?

$$
\begin{aligned}
(m^e \bmod N)^d \bmod N &= m^{ed} \bmod N \\
&= m^{1+t\phi(N)} \bmod N \\
&= m^1 \cdot \left(m^{\phi(N)}\right)^t \bmod N
\end{aligned}
$$

Why Does It Work?

$$\begin{aligned}(m^e \bmod N)^d \bmod N &= m^{ed} \bmod N \\ &= m^{1+t\phi(N)} \bmod N \\ &= m^1 \cdot \left(m^{\phi(N)}\right)^t \bmod N \\ &= m \cdot 1^t \bmod N\end{aligned}$$

Why Does It Work?

$$
\begin{aligned}
(m^e \bmod N)^d \bmod N &= m^{ed} \bmod N \\
&= m^{1+t\phi(N)} \bmod N \\
&= m^1 \cdot \left(m^{\phi(N)}\right)^t \bmod N \\
&= m \cdot 1^t \bmod N \\
&= m \bmod N
\end{aligned}
$$