Lecture 5

Douglas Wikström
KTH Stockholm
dog@csc.kth.se

February 20, 2015

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

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

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 $0 < a < n$ relatively prime to n.

Euler's Phi-Function (Totient Function)

Definition. Euler's Phi-function $\phi(n)$ counts the number of integers $0 < a < n$ relatively 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 $0 < a < n$ relatively 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 $0 < a < n$ relatively 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 $0 < a < n$ relatively 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 $b^{\phi(n)} = 1 \bmod n$.

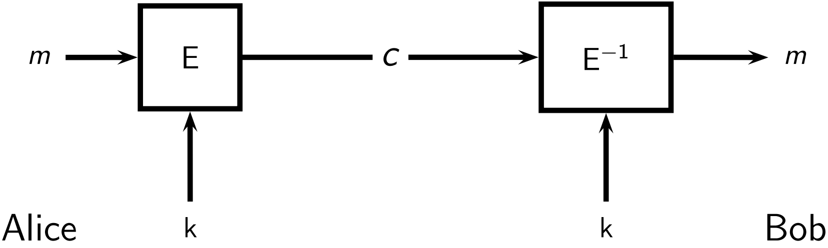
Multiplicative Group of a Prime Order Field

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.

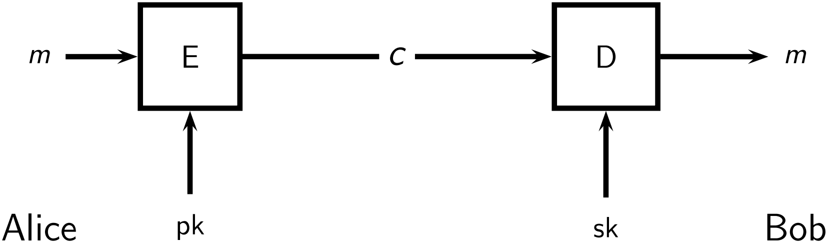
Cipher (Symmetric Cryptosystem)

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



Public-Key Cryptosystem

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



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 $(\mathsf{pk}, \mathsf{sk})$ and $m \in \mathcal{M}_{\mathsf{pk}}$.