CS 4770: Cryptography

CS 6750: Cryptography and Communication Security

Alina Oprea
Associate Professor, CCIS
Northeastern University

March 15 2018

Review

- Hash functions
  - Collision resistance
  - Merkle-Damgaard construction
- Birthday attacks on hash functions
  - Upper and lower bound on collision probability
- MAC constructions
  - MACs from hash functions
  - HMAC construction
  - More efficient than CBC-MAC

Number theory review

Greatest common divisor

Def: For integers x, y: **gcd(x, y)** is the *greatest common divisor* d such that $d|x$ and $d|y$

Fact: for all integers x, y there exist a, b such that

$$a \cdot x + b \cdot y = \gcd(x,y)$$

Coef a,b can be found with *extended Euclidean algorithm*

If $\gcd(x,y)=1$ we say that x and y are **relatively prime**

Fact: x and y are relatively prime if and only if there exist a, b such that

$$a \cdot x + b \cdot y = 1$$

Modular inversion

Over rationals, inverse of 2 is ½ . What about Z_N ?

Definition: The **multiplicative inverse** of x in Z_N is an element y in Z_N such that $x \cdot y = 1$ in Z_N

y is denoted x^{-1}

Example: Let N be an odd integer. What is the inverse of 2 in Z_N?

$$2 \cdot \frac{N+1}{2} = \mathrm{N} + 1 = 1 \bmod \mathrm{N}$$

Modular inversion

Which elements have an inverse in Z_N?

Lemma: x in Z_N has an inverse if and only if gcd(x,N) = 1

Proof:

- gcd(x,N)=1 $\Rightarrow$ $\exists$ a,b: $a \cdot x + b \cdot N = 1$

  $a \cdot x = 1 \bmod N \Rightarrow x^{-1} = a$

- If x has an inverse a $\Rightarrow$ $a \cdot x = 1 \bmod N \Rightarrow$ exists b $a \cdot x = bN + 1 \Rightarrow a \cdot x - bN = 1 \Rightarrow \gcd(x,N) = 1$

Solving modular linear equations

Solve: **$a \cdot x + b = 0$** in Z_N

Solution: **$x = -b \cdot a^{-1}$** in Z_N

only if a is invertible

Find a^{-1} in Z_N using extended Euclidean alg.

Run time: $O(\log^2 N)$

Groups

- **Definition**: A *group* (G, *) is a set G on which a binary operation is defined which satisfies the following properties:
  - *Closure*: For all a, b ∈ G, a * b ∈ G.
  - *Associative*: For all a, b, c ∈ G, (a * b)* c = a * (b * c).
  - *Identity*: ∃ e ∈G s.t. for all a ∈ G, a* e = a = e * a.
  - *Inverse*: For all a ∈ G, ∃ a^{-1} ∈ G s. t. a* a^{-1} = a^{-1}* a=e.
- Examples
  - (Z_N,+) is a group, where + is addition modulo N
  - (Z_p,*) is a group, where * is multiplication modulo p

Abelian and cyclic groups

- **Definition**: A group (G, *) is called *abelian* if operation * is commutative
  - *Commutative*: For all a, b ∈ G, a * b = b * a
- Example: $(Z_N,+)$ is an abelian group
- **Definition**: A group G is *cyclic* if ∃ generator g ∈G s.t. any h ∈G can be writen h = g^i
- Example: $(Z_p,*)$ is a cyclic group

Invertible elements in Z_N

Definition (*group of invertible elements* in Z_N)

$$\mathbb{Z}_N^* = \{ x \in Z_N : \gcd(x,N) = 1 \}$$

Examples:

1. for prime p,

$$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$$

2. $\mathbb{Z}_{12}^* = \{ 1, 5, 7, 11\}$

For x in $\mathbb{Z}_N^*$, can find x^{-1} using extended Euclidean algorithm

Order of group/elements

- **Definition**: The *order of a group* G, ord(G), is defined as the number of elements in the group.
- Example: The order of $(Z_p,*)$ is p-1
- **Definition**: The *order of an element* g from a finite group G, is the smallest power of n such that $g^n=e$, where e is the identity element.
- Example: What is the order of 2 in $(Z_5^*, *)$?
  - It is 4 because $2^4 \equiv 1 \bmod 5$

Facts on group order

Theorem: If G is a group of order m. Then for any element $g \in G$, $g^m = 1$.

Proof (assume G abelian): Let $g_1,\ldots,g_m$ be all the elements of G and g an element in G. Then:

$$g_1 \cdot \ldots \cdot g_m = (g \cdot g_1) \ldots (g \cdot g_m)$$

This is true because all m elements on the right side of the equality are distinct.

Then: $g_1 \cdot \ldots \cdot g_m = g^m g_1 \cdot \ldots \cdot g_m$ and thus $g^m = 1$

Computing in the exponent

Theorem: Let G be a group of order m. Then for any element $g \in G$, $g^m = 1$.

Corollary Let G be a group of order m>1. Then for any element $g \in G$ and any integer x:

$$g^x = g^{[x \bmod m]}$$

Fermat's Little Theorem

Theorem: Let G be a group of order m. Then for any element g ∈ G, $g^m = 1$.

Corollary Let p be a prime. For any integer a:

$$a^{p-1} = 1 \bmod \mathrm{p}$$

Proof:

Apply the theorem for $(Z_p^*, *)$. The order of Z_p^* is p-1 and the result follows immediately.

The structure of Z_p^*

Theorem: Z_p^* is a cyclic group, that is

$\exists$ g $\in Z_p^*$ such that $\{1, g, g^2, \ldots, g^{p-2}\} = Z_p^*$

g is called a generator of Z_p^*

Example (p=7):

$\{1, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = Z_7^*$

Not every element is a generator

$\{1, 2, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$

Euler's generalization of Fermat (1736)

Definition: For an integer N define $\phi(N) = |Z_N^*|$

Examples:

- $\phi(p) = p-1$ for p prime
- $\phi(12) = |\{1,5,7,11\}| = 4$
- For $N=p\cdot q$, p and q primes, $\phi(N) = (p-1)(q-1)$
  - Num. elements divisible with p is q-1
  - Num. elements divisible with q is p-1
  - $\phi(N) = N-1-(p-1)-(q-1) = (p-1)(q-1)$

Euler's Theorem

Theorem: Let G be a group of order m. Then for any element $g \in G$, $g^m = 1$.

Corollary For any integer a:

$$a^{\phi(N)} = 1 \bmod \mathrm{N}$$

Proof:

Apply the theorem for $(Z_N^*, *)$. The order of Z_N^* is $\phi(N)$ and the result follows immediately.

Example: $5^{\phi(12)} = 5^4 = 625 = 1$ in Z_{12}^*

Basis of the RSA cryptosystem

Modular e'th roots

We know how to solve modular **linear** equations:

$\mathbf{a \cdot x + b = 0}$ in Z_N Solution: $\mathbf{x = -b \cdot a^{-1}}$ in Z_N

What about higher degree polynomials?

Example: Let p be a prime and $c \in Z_p$.

Can we solve:

$x^2 - c = 0$, $y^3 - c = 0$, $z^{37} - c = 0$ in Z_p

Modular e'th roots

Let p be a prime and $c \in Z_p$.

Definition: $x \in Z_p$ s.t. $X^e = c$ in Z_p is called an *e'th root* of c .

Examples:

$7^{1/3}$ = 6 in $\mathbb{Z}_{11}$

$6^3 = 216 = 7 \; mod \; 11$

$3^{1/2}$ = 5 in $\mathbb{Z}_{11}$

$1^{1/3}$ = 1 in $\mathbb{Z}_{11}$

$\boxed{2^{1/2} \text{ does not exist in } \mathbb{Z}_{11}}$

The easy case

When does **$c^{1/e}$ in** Z_p^* exist? Can we compute it efficiently?

<u>**The easy case**</u>: suppose gcd(e , p-1) = 1

Then for all c in Z_p^* : **$c^{1/e}$** exists in Z_p^* and is easy to find.

Proof: There exists a and b s.t. a·e + b(p-1)= 1.

c $= \; c^{ae+b(p-1)} = c^{ae}(c^{p-1})^b = c^{ae}$. Then c^a is the e-th root of c

The case e=2: square roots

If p is an odd prime then gcd(2, p-1) ≠ 1

$$x \qquad -x$$
$$\searrow \quad \swarrow$$
$$x^2$$

Fact: in Z_p^* , x ⟶ x^2 is a 2-to-1 function

Example: in Z_{11}^* :

1 10	2 9	3 8	4 7	5 6
1	4	9	5	3

Definition: x in Z_p^* is a **quadratic residue** (Q.R.) if it has a square root (exists y in in Z_p^* such that $y^2 = x$ mod p)

p odd prime ⇒ the # of Q.R. in is (p+1)/2

Q.R. theorem for odd primes

Theorem: Let p be an odd prime. Then x in Z_p^* is a Q.R. $\Longleftrightarrow$ $x^{(p-1)/2} = 1 \bmod p$

Example:

in $\mathbb{Z}_{11}$:	1^5,	2^5,	3^5,	4^5,	5^5,	6^5,	7^5,	8^5,	9^5,	10^5
=	1	-1	1	1	1,	-1,	-1,	-1,	1,	-1

Proof: If x is Q.R., there exists y such that:

$y^2 = x \; mod \; p$. Then $x^{\frac{p-1}{2}} = \mathrm{y}^{\mathrm{p}-1} = 1 \bmod \mathrm{p}$

Q.R. theorem for odd primes

Theorem: Let p be an odd prime. Then x in Z_p^* is a Q.R. $\iff$ $x^{(p-1)/2} = 1 \bmod p$

Proof: Let p = 3 mod 4. Assume $x^{\frac{p-1}{2}} = 1 \bmod \mathrm{p}.$

Then: $\left[x^{\frac{p+1}{4}}\right]^2 = x^{\frac{p+1}{2}} = x^{\frac{p-1}{2}} x = x$

So $x^{\frac{p+1}{4}}$ is the square root of x, and thus x is Q.R.

Proof can be extended to p = 1 mod 4.

Solving quadratic equations mod p

Solve: $\mathbf{a \cdot x^2 + b \cdot x + c = 0 \quad in \quad Z_p}$

Solution: $\mathbf{x = \quad (-b \pm \sqrt{b^2 - 4 \cdot a \cdot c}\ ) \ / \ \ 2a \quad in \quad Z_p}$

- Find **$(2a)^{-1}$ in Z_p** using extended Euclidean alg.
- Find square root of **$b^2 - 4 \cdot a \cdot c$** in Z_p (if it exists) using a square root algorithm

Computing e'th roots mod N ??

Let N be a composite number and e > 1

When does **$c^{1/e}$ in Z_N** exist? Can we compute it efficiently?

Answering these questions requires the factorization of N

(as far as we know)

Intractable problems with composites

Consider the set of integers: (e.g., for n=1024)

$$C(n) := \{ N = p \cdot q \quad \text{where } p,q \text{ are n-bit primes} \}$$

Problem 1: Factor a random N in C(n) (for large n=1024)

Problem 2: Given a polynomial **f(x)** where degree(f) > 1 and a random N in C(n) find x in s.t. f(x) = 0 mod N

RSA assumption: Taking modular roots $\mathbf{c^{1/e}}$ **in** $\mathbf{Z_N}$ for e>2 is hard

Factoring assumption is weaker than RSA

The factoring problem

Gauss (1805): *"The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic."*

Best known alg. (NFS): run time exp($\tilde{O}(\sqrt[3]{n})$) for n-bit integer

Current world record: **RSA-768** (232 digits)

- Work: two years on hundreds of machines
- Factoring a 1024-bit integer: about 1000 times harder

$\Rightarrow$ likely possible this decade

Key insights

- Numbers have a unique factorization into primes
- Solving linear equations in Z_N can be done efficiently with extended Euclidian algorithm
- Solving quadratic equations in Z_p^* can be done efficiently
- Computing modular roots mod N (for N a random large number N=pq, p, q primes) is considered an intractable problem
  - Basis of RSA algorithm

Further reading

- A Computational Introduction to Number Theory and Algebra,
  V. Shoup, 2008   (V2),   Chapter 1-4, 11, 12

  Available at **//shoup.net/ntb/ntb-v2.pdf**

How to generate large primes?

- Input: length n; parameter t
- Output: a uniform n-bit prime p
- For i = 1 to t:
  - $p' \leftarrow \{0,1\}^{n-1}$
  - $p = 1||p'$
  - If p is prime, return p

Primality test

- Return fail

The fraction of prime n-bit numbers is > 1/3n

Set t to get a negligible prob of fail (e.g., for $t=3n^2$, probability of failure $< e^{-n}$)

Primality testing – Attempt I

- **Goal**: Distinguish primes from composites
  - Test input number N
- If N is prime, then for all $a \in \{1, \dots, N-1\}$, $a^{N-1} = 1 \bmod N$ (Fermat's theorem)
- If there *exists an a* for which $a^{N-1} \neq 1 \bmod N$, then N is composite
- Such an a is called a *witness* for N composite
- If there exists a witness a, then at least half elements in Z_N^* are witnesses for N composite
  - Some composites do not have witnesses!

Primality testing – Refined

- **Goal**: Distinguish primes from composites
  - Test input number N
- If N is even, it is composite
- If N is perfect power ($N = m^e$), it is composite
- Otherwise, decompose $N - 1 = 2^r u$, u odd
- An a is called *strong witness* if:
  - $a^u \neq \pm 1 \; mod \; N$ and
  - $a^{2^i u} \neq -1 \; mod \; N, \forall i \in \{1, \ldots, r-1\}$
- If N is composite, then at least half elements in Z_N^* are strong witnesses!

Miller-Rabin primality test

- Input: Integer N; parameter t
- Output: A decision whether N is prime/composite
- If N even, return "composite"
- If N perfect power, return "composite"
- Decompose $N - 1 = 2^r u$, u odd
- For j = 1 to t:
  - $a \leftarrow$ {1,…,N-1} // choose at random
  - If $a^u \neq \pm 1 \bmod N$ and $a^{2^i u} \neq -1 \bmod N, \forall i \in \{1, \ldots, r-1\}$, return "composite"
- Return "prime"

If N composite, prob ½ to find strong witness in each iteration
If N composite, the probability that it outputs prime is $1/2^t$

Acknowledgement

Some of the slides and slide contents are taken from
http://www.crypto.edu.pl/Dziembowski/teaching
and fall under the following:

We have also used slides from Prof. Dan Boneh online cryptography course at Stanford University:

http://crypto.stanford.edu/~dabo/courses/OnlineCrypto/