CSC3631 Cryptography
- Number Theory & Algebra II

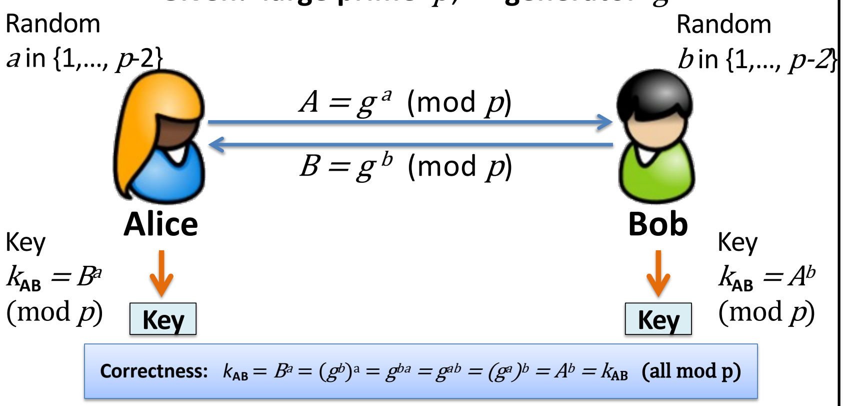
Thomas Gross

Review Secure Channels

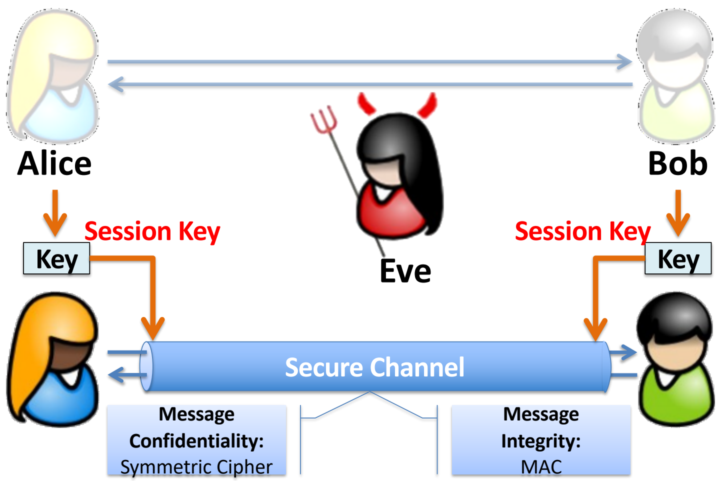
- What are secure channel examples used in daily life?
- What are secure channels good for?

Review: Diffie-Hellman in $(\mathbf{Z}_p)^*$

Given: large prime p; **generator** g



Creating a Secure Channel



Key Derivation and Channel Creation

K **Session Key** Random salt

Key Derivation Function

Extract-then-Expand

$K_{ext} \leftarrow$ **HMAC**(salt, K)

$K_i \leftarrow$ **HMAC**(K_{ext}, i) **(Use as PRF)**

$k_{MAC,\,AB}$ $k_{MAC,\,BA}$ $k_{ENC,\,AB}$ $k_{ENC,\,BA}$

8

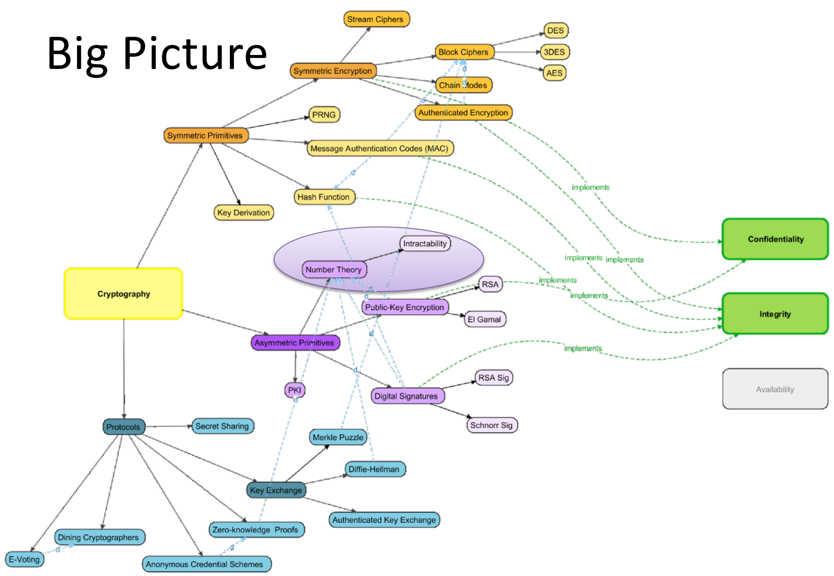
Quick Review Number Theory

N: positive integer p: prime number

- $\mathbf{Z}_N$: set of integers { 0, 1, …, N-1 }
  - Modular arithmetic (+, ·) works as expected.
- **gcd**(x, y) = $a \cdot x + b \cdot y$ **solved with EEA**
- **Modular inverse:** $y = x^{-1}$ $x \cdot y = 1 \pmod N$
- Exists if **gcd**(x, N) = 1 **solved with Euclid**
- ($\mathbf{Z}_N$)*: set of invertible elements in $\mathbf{Z}_N$
- ($\mathbf{Z}_p$)*: **cyclic group**, with some **generator** g

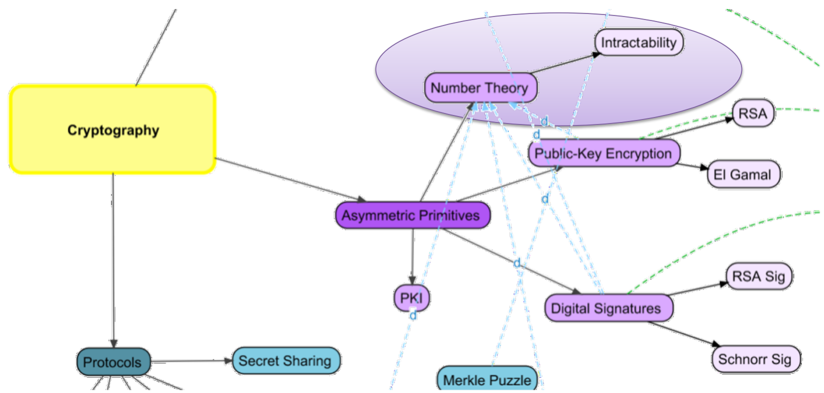
9

Big Picture



10

Big Picture



11

Roadmap

- Fermat's Theorem
- Application: Generating large random primes
- Group Order and Euler' Theorem
- Computing the eth root

Goal for today: Establish the basis for

- **The asymmetric RSA encryptions and signatures, and**
- **Hard problems in asymmetric crypto.**

Foundational Laws

How to cancel out values?

Fermat	Euler	eth Root
$x^{p-1} = 1$ (mod p)	$x^{\varphi(N)} = 1$ (mod N)	$x^{1/e}$? (mod p)
$\mathbf{Z}_p$	$\mathbf{Z}_N$	$\mathbf{Z}_p$
Gen Primes	RSA Crypto	RSA Crypto

Invertible Elements in $\mathbf{Z}_N$

Recall: What's the environment for asymmetric crypto?

$(\mathbf{Z}_N)^*$ = { invertible elements in $\mathbf{Z}_N$ }
= { elements in $\mathbf{Z}_N$ **coprime** to N }
= { x in $\mathbf{Z}_N$: **gcd**$(x, N) = 1$ }

Example: $(\mathbf{Z}_{14})^*$ = { 1, 3, 5, 9, 11, 13 }

If p is **prime,** then $(\mathbf{Z}_p)^*$ is $\mathbf{Z}_p \setminus \{0\}$
In $\mathbf{Z}_p$ all elements apart from 0 are invertible.

The Structure of $(\mathbf{Z}_p)^*$

The set of invertible elements of $\mathbf{Z}_p$ is **cyclic**.

$(\mathbf{Z}_p)^*$ is a **cyclic group**
Exists a g in $(\mathbf{Z}_p)^*$ such that
$\{1, g, g^2, g^3, \dots g^{p-2}\} = (\mathbf{Z}_p)^*$
We call g a **generator** of $(\mathbf{Z}_p)^*$

Example p=5: $\{1, 3, 3^2, 3^3\} = \{1, 3, 4, 2\} = (\mathbf{Z}_5)^*$

Fermat's Theorem

Theorem:
For all x in $(\mathbf{Z}_p)^*$

$$x^{p-1} = 1 \quad (\textbf{mod } p)$$

Example: $p=7$ $(\mathbf{Z}_p)^* = \{1, 2, 3, 4, 5, 6\}$

x^{p-1} (mod p)	2^6 (mod 7)	3^6 (mod 7)	4^6 (mod 7)	5^6 (mod 7)	6^6 (mod 7)
Congruent to	64 (mod 7)	729 (mod 7)	4096 (mod 7)	15625 (mod 7)	46656 (mod 7)
	1 (mod 7)	1 (mod 7)	1 (mod 7)	1 (mod 7)	1 (mod 7)

Fermat-Application I: Inverses in $(\mathbf{Z}_p)^*$

Recall: x^{-1} is inverse of x if $x \cdot x^{-1} = 1 \quad (\textbf{mod } p)$

Fermat: $x^{p-1} = 1 \quad (\textbf{mod } p)$

In $(\mathbf{Z}_p)^*$ the **inverse** is: $x^{-1} = x^{p-2}$ (**mod** p)

Roadmap

- Fermat's Theorem
- **Application: Generating large random primes**
- Group Order and Euler' Theorem
- Computing the eth root

Goal for today: Establish the basis for

- **The asymmetric RSA encryptions and signatures, and**
- **Hard problems in asymmetric crypto.**

Fermat-Application II: Generate Primes

How can we generate the huge primes used in crypto?

Goal: Generate random prime p 2048 bits

Choose a random integer p w/ 2048 bits

k times:
For a random witness $\boldsymbol{a}$ in $\mathbf{Z}_p$:
Test $a^{p-1} \overset{?}{==} 1 \quad (\textbf{mod } p)$?

True for all *k tests*: return p (as probable prime)

Any false: restart (eliminated p)

Review Fermat

Fermat

$x^{p-1} = 1$ (mod p)

Z_p

Gen Primes

Inverse in $(Z_p)^*$

$X^{-1} = x^{p-2}$ (mod p)

Generate Primes

$a^{p-1} = 1$? (mod p)

Roadmap

- Fermat's Theorem
- Application: Generating large random primes
- **Group Order and Euler' Theorem**
- Computing the e^{th} root

Goal for today: Establish the basis for
- **The asymmetric RSA encryptions and signatures, and**
- **Hard problems in asymmetric crypto.**

Euler's phi Function

What do we need to build up Euler's theorem?

Euler's phi function (**Euler's totient function**)

For all positive integers N

$$\varphi(N) := |(\mathbf{Z}_N)^*| \qquad \text{(the size of } (\mathbf{Z}_N)^*)$$

$\varphi(N)$ = number of elements in $\mathbf{Z}_N$ **coprime** to N
= number of invertible elements in $\mathbf{Z}_N$
= the group order of $(\mathbf{Z}_N)^*$

Cf. Shoup2008, Chapter 2.6

How to compute $\varphi(N)$?

- **Easy**, if prime factorization of N is known:
$$N = p_1^{e_1} \ldots p_k^{e_k}$$
- Then, $\varphi(N) = \prod(\varphi(p_1^{e_1}) \ldots \varphi(p_k^{e_k}))$.
- For a prime factor p and integer e:
$$\varphi(p^e) = p^{e-1}(p-1)$$
- **Intractable**, if prime factorization of N unknown.

Order of an Element I

For a in $(\mathbf{Z}_N)^*$, the order of a is the smallest c, such that

$$a^c = 1 \qquad (\textbf{mod } N)$$

What does that mean?

Order of an Element II

Recall: A **generator** g in $(\mathbf{Z}_p)^*$ generates a group $\{1, g, g^2, g^3, \ldots\}$

We call the group generated by g: <g>

Order of g in $(\mathbf{Z}_p)^*$ is the size of the generated group <g>.

$$\textbf{ord}(g) := |\langle g \rangle|$$

Example p=5, g=3: $\{1, 3, 3^2, 3^3\} = (\mathbf{Z}_5)^*$ → $\textbf{ord}(g) = 4$

Euler's Theorem

Theorem:
For all integers x in $(Z_N)^*$ holds:

$$x^{\varphi(N)} = 1 \quad (\text{mod } N)$$

In particular, the order of any element x in $(Z_N)^*$ divides $\boldsymbol{\varphi}(N)$.

Why does that matter?
Knowing the group order $\boldsymbol{\varphi}(N)$ allows you to

- Cancel out elements x by raising it to $\boldsymbol{\varphi}(N)$ and
- resolve computations that are otherwise hard.

Finding a Generator of a Cyclic Group G with Order n (e.g., Group of $(\mathbf{Z}_N)^*$)

$\langle g \rangle = G$ if $\textbf{ord}(g) = n$

⇔ Smallest c, s.t. $g^c = 1$ (mod N), equals n.

Exist $\boldsymbol{\varphi}(n)$ generators of a cyclic group G with order n.

Assume prime factorization of n known: $n = p_1^{e_1} \ldots p_k^{e_k}$.

1. Choose random element g of G.
2. For $i = 1$ to k do:
   - Compute $b \leftarrow g^{n/p_i}$ (mod N)
   - If $b = 1$ then goto Step 1.
3. Return g

Review Euler

Euler

$x^{\varphi(N)} = 1$ **(mod N)**

$\mathbf{Z}_N$

RSA Crypto

Order of $(\mathbf{Z}_N)^*$

$\varphi(N) := |(\mathbf{Z}_N)^*|$

(Number of elements)

Knowing $\varphi(N)$

Gives us an advantage against an adversary.

Roadmap

- Fermat's Theorem
- Application: Generating large random primes
- Euler' Theorem
- **Computing the eth root**

Goal for today: Establish the basis for

- **The asymmetric RSA encryptions and signatures, and**
- **Hard problems in asymmetric crypto.**

eth Root in $(\mathbf{Z}_p)^*$

How is the eth root defined?

The eth root of c is the x in $(\mathbf{Z}_p)^*$, such that

$$x^e = c \qquad (\textbf{mod } p)$$

We write the eth root $c^{1/e}$.

Examples: p=7

$2^{1/2} = 3$ in $(\mathbf{Z}_7)^*$

$6^{1/3} = 3$ in $(\mathbf{Z}_7)^*$

How hard is computing the eth Root?

In $(\mathbf{Z}_p)^*$: Easy if gcd(e, p-1) = 1

- **Choose $d = e^{-1}$ in $\mathbf{Z}_{p-1}$** $\rightarrow$ $d \cdot e = 1$ **in $\mathbf{Z}_{p-1}$**
- $(c^d)^e = c^{d \cdot e} = c^{k(p-1)+1} = [c^{p-1}]^k \cdot c = c$

In $(\mathbf{Z}_N)^*$: Hard

Believed to require factorization of N

Review e^{th} Root

e^{th} Root

$x^{1/e}$?
(mod p)

Z_p

RSA Crypto

e^{th} root in $(Z_p)^*$: easy

IF we can invert *e* mod *p*-1
gcd(*e*, *p*-1) = 1

e^{th} root in $(Z_N)^*$: hard

Probably requires factorization of *N*

Problem Structure

The Big Showdown: How to cancel out values?

Fermat	Euler	e^{th} Root
$x^{p-1} = 1$ (mod p)	$x^{\varphi(N)} = 1$ (mod N)	$x^{1/e}$? (mod p)
Z_p	Z_N	Z_p
Gen Primes	RSA Crypto	RSA Crypto