VE475 Mid Review

Before the Review

- Part A
  - Closed book
  - Reviewed during the lecture
  - Concepts & memorization

Before the Review

- Part B
  - Open book (**ONLY** printed/electronic slides + notes)
  - Calculation (calculators not needed)
  - Mathematical proof (Similar to homework)
  - ~ch04

Chapter 1 - Overview

Chapter 1

- What's Eve's strategy?
  - Ciphertext only/KPA/CPA/CCA/CPCA !
  - CPA1/CPA2/Adaptive? !
- What is *Kerckhoffs' principle*?
- What is *Caesar cipher*? How to attack?

Greatest Common Divisor

What is *Bézout's identity*?

Greatest Common Divisor

What is *Bézout's identity*?

If $d = gcd(a, b)$, then there exists s and t, such that $as + bt = d$.

What is **Extended Euclidean Algorithm** ! !

- What is $11111^{-1} \mod 12345$?

Invertible?

- GCD(a, b) = 1 $\approx a \neq 0$.

Compute $gcd(30030, 257)$ -> 257 is prime.

Modern Cryptography

- Symmetric or Asymmetric
  - What is the issue?
- Public Key Cryptography
  - General idea?

Measuring Security

- Key space?
- Computational complexity
  - 2^{128} or 128 bit security ! !
- Meet in the middle
  - Security in double encryption?

Zero knowledge Proof

- What is the general idea (Bob's secret door key)?
- Probability problem ! !
- Not related to computational power

Chapter 2 - Block Ciphers

Block Ciphers

- Mode?
  - ECB/CBC/CTR
- What is true *randomness*?
  - *Kolmogorov randomness* (incompressible)
- BBS generator
  - Why secure?
  - *Quadratic Residuosity (QR)* Problem

Fermat's Little Theorem ! !

What is FLT?

If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$.
More generally, $a^p \equiv a \mod p$.

Square roots modulo a prime

Let $p \equiv 3 \mod 4$ be a prime, $x \equiv y^{\frac{p+1}{4}} \mod p$.
If y has a square root mod p, $(\pm x)^2 \equiv y \mod p$,
else $(\pm x)^2 \equiv -y \mod p$.

Chinese Remainder Theorem ! !

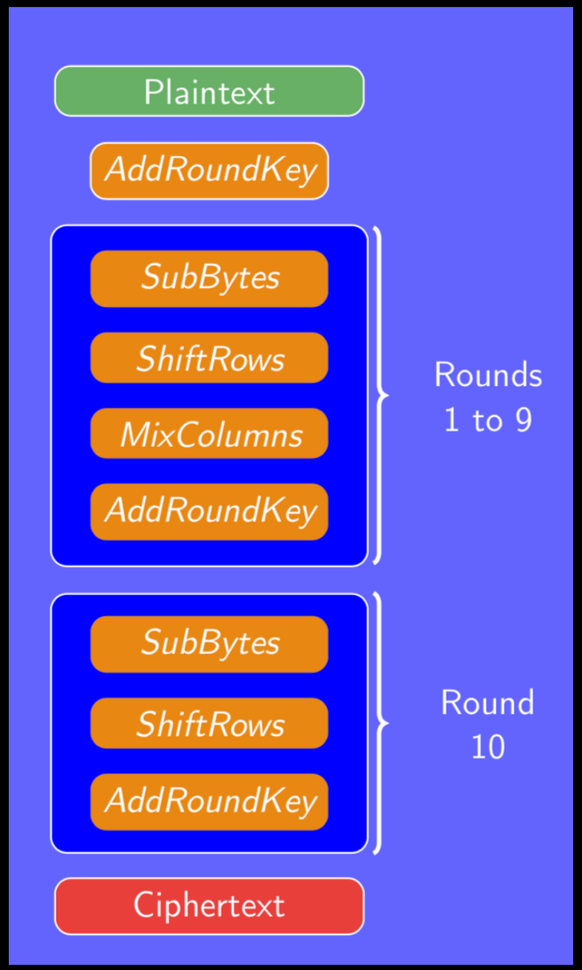
Find x such that $x_2 \equiv 71 \mod 77$

Find $2^{2017} \mod 2015$.

Basic Feistel network

- What is *Feistal Network? How does it work*?
- How to generally attack *Feistal Network*?

Advanced Encryption Standard (AES)



Non-prime Fields ! !

How to construct a finite field of 9 elements?

$$\mathbb{F}_3[X]/ < \text{irreducible polynomial with degree of } 2 >$$

or simply $\mathbb{F}_{3^2}[X]$.

What is the polynomial? Write out all elements?

Chapter 3 - Public Key Cryptography

One-way Function

- easy to evaluate but hard to invert
- injective
- easy to invert with the knowledge of a trapdoor

Group ! !

+/-

- Associativity
- Existence of a unit element
- Existence of inverse
- Commutativity -> Abelian

Ring

+/- & $\times$

- Abelian
- Multiplicative unit
- Associativity
- Distributivity

Field ! !

+/- & $\times/\div$

- $0 \neq 1$
- $a \cdot a^{-1} = 1$ for every $a \in F$ except 0.

Order ! !

- Order of a group: cardinality
- Order of an element: $g^m = 1$.
- *Primitive element* of a group or a *generator*.

Euler's Totient Function ! !

For any prime p,

$$\varphi(p^k) = p^{k-1}(p-1)$$

and

$$\varphi(n) = n\prod_{p|n}(1-\frac{1}{p})$$

Lagrange's Theorem

Any element x of G divides the order of G.

Euler's Theorem ! !

a, n coprime => $a^{\varphi(n)} \equiv 1 \mod n.$

Calculate $2^{639613} \mod 5353.$

Finding generators

What is the property of a generator?

How to use the property of generator / its order?

- ORDER -> FACTORIZATION: easy
- FACTORIZATION -> ORDER: easy
- Factorization: hard
- Order: hard

Legendre Symbol

check if an element is a square modulo a prime.

Is 12 a square mod 31?

Jacobi Symbol !

Calculate $(\frac{4567}{12345})$.

- $(\frac{a}{n}) = -1$: a is not a square mod n.

RSA Cryptosystem

Modular exponentiation

Square and multiply algorithm for efficient *exp*.

Generating Prime numbers

- How to get a prime?
- How to check the primality
  - The Solovay-Strassen primality test
  - The Miller-Rabin primality test
- What if non-prime is taken?

How to factorize?

Pollard's Rho Algorithm.

- Into a cycle
- Use the property of the cycle
- How to compute the complexity to gain a certain probability?

More on RSA

The Discrete Logarithm Problem

Again, *Pollard's Rho Algorithm*.

What's the relation between DLP and factorization/order?

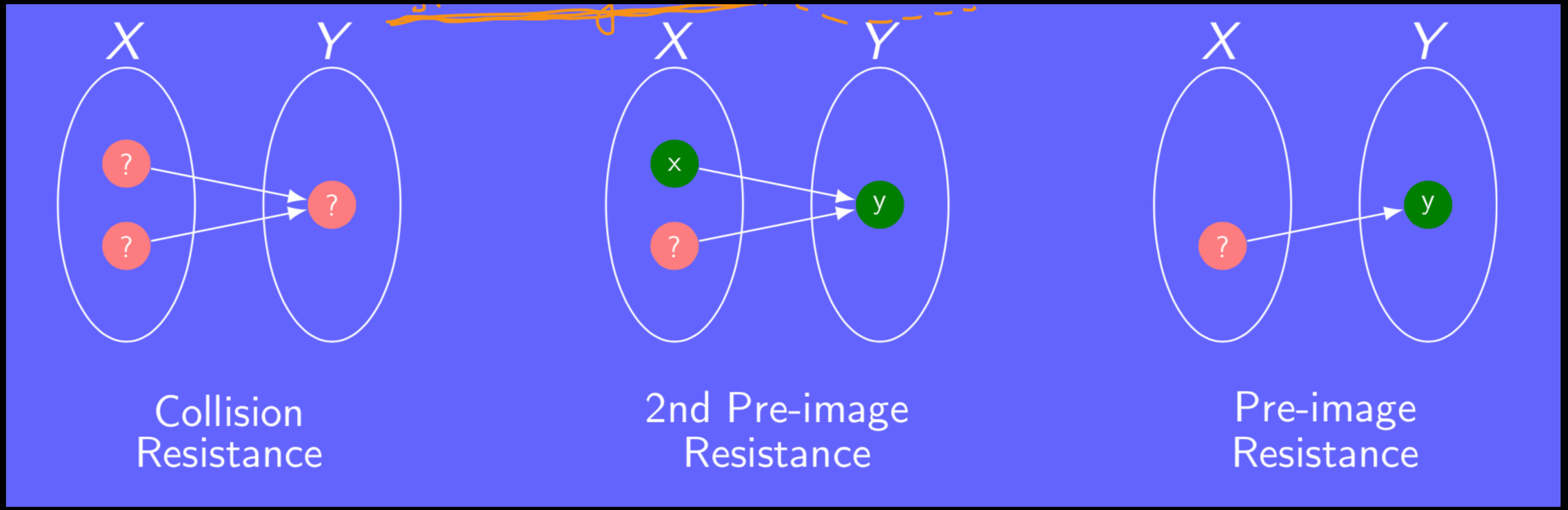
Diffie-Hellman key exchange

Elgamal & CDH/DDH

Chapter 4 - Hash Functions

Hash functions !

Efficiently & any input



DLP Hash Function

Why would that work?

Birthday Attack ! !

Complexity of around $\mathcal{O}(\sqrt{n})$

What about real day?

Merkle-Damgård theorem

SHA-1