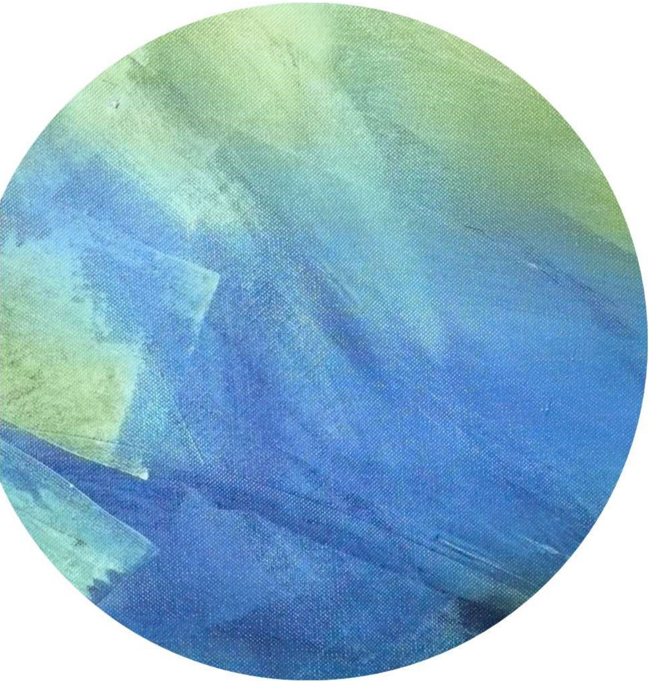
Lecture 8



Outline

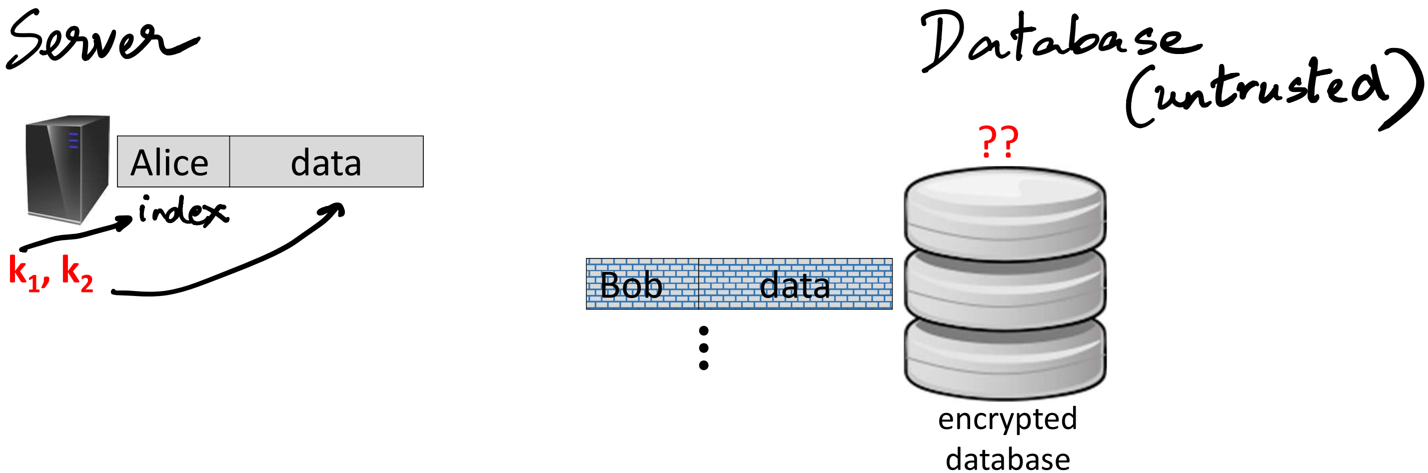
Deterministic Encryption

Format-Preserving Encryption

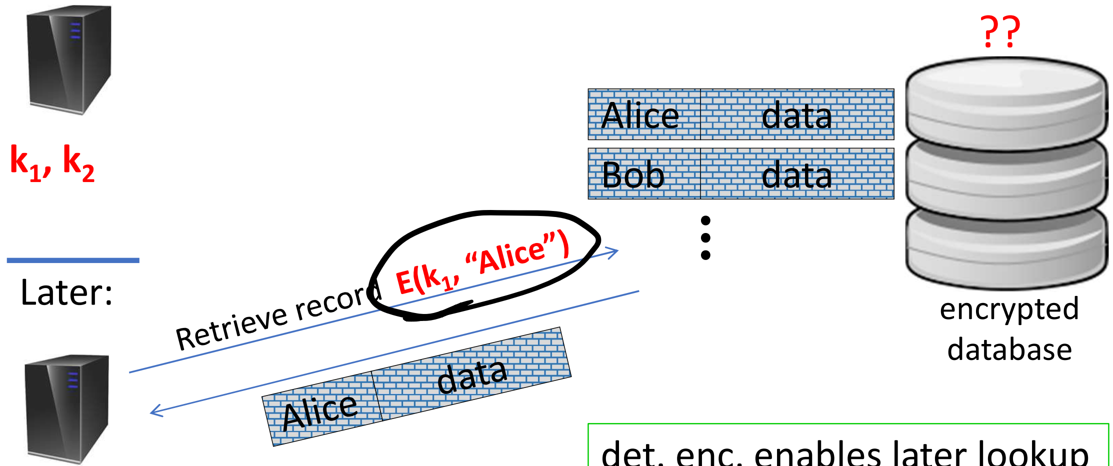
Number Theory

Deterministic Encryption

Deterministic Encryption



Deterministic Encryption

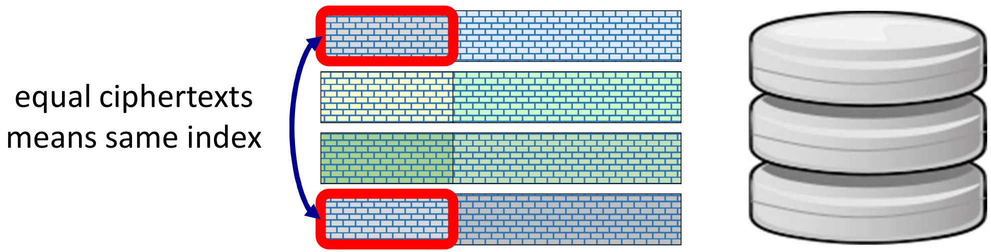


det. enc. enables later lookup

Deterministic Encryption

The problem: attacker can tell when two ciphertexts encrypt the same message $\Rightarrow$ leaks information

Leads to significant attacks when message space M is small.

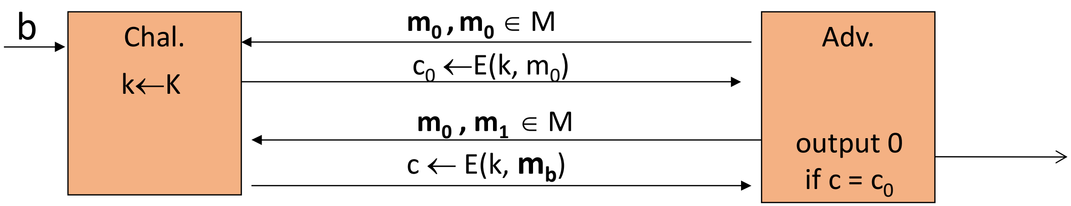


Deterministic Encryption is NOT CPA-Secure

The problem: attacker can tell when two ciphertexts encrypt the same message $\Rightarrow$ leaks information

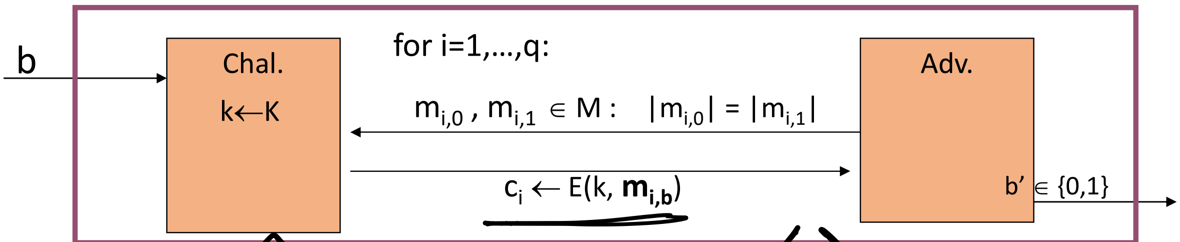
Leads to significant attacks when message space M is small.

Attacker wins CPA game: (Adaptive CPA)



Deterministic Encryption

$\mathbb{E} = (E,D)$ a cipher defined over (K,M,C). For bit b define EXP(b) as:



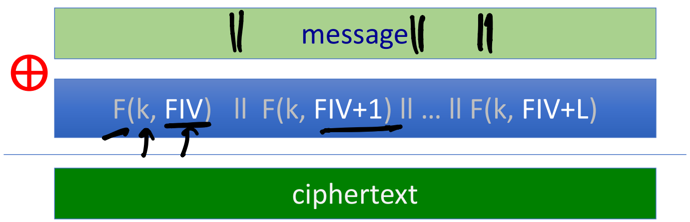
where $\mathbf{m_{1,0}, \ldots, m_{q,0}}$ are distinct and $\mathbf{m_{1,1}, \ldots, m_{q,1}}$ are distinct

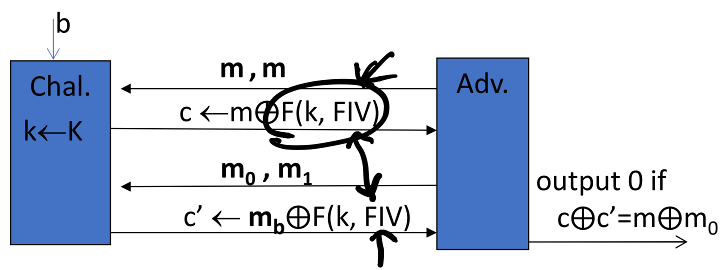
Def: $\mathbb{E}$ is **sem. sec. under det. CPA** if for all efficient A:

$$\mathrm{Adv}_{\mathrm{dCPA}}[A,\mathbb{E}] = \big| \Pr[\mathrm{EXP}(0)=1] - \Pr[\mathrm{EXP}(1)=1] \big| \quad \text{is negligible.}$$

IV is set to a fixed string.
(not randomized)

Is counter mode with a fixed IV det. CPA secure?





Derive IV as det. function of msg.

Construction: Synthetic IV (SIV)

Let (E, D) be a CPA-secure encryption. $\mathbf{E(k, m \; ; \; \underset{\downarrow \text{IV}}{r}) \longrightarrow c}$

Let $F: K \times M \longrightarrow R$ be a secure PRF

Define: $\mathbf{E_{det}((k_1,k_2) , m) =}$ First compute $\overset{\text{IV}}{r} = F(k_2, m)$
Output $E(k_1, m; r)$ ← separates randomness from inputs

Thm: $\mathbf{E_{det}}$ is sem. sec. under det. CPA .

Proof sketch: distinct msgs. ⇒ all r's are indist. from random

Well suited for messages longer than one AES block (16 bytes)

Deterministic Authenticated Encryption

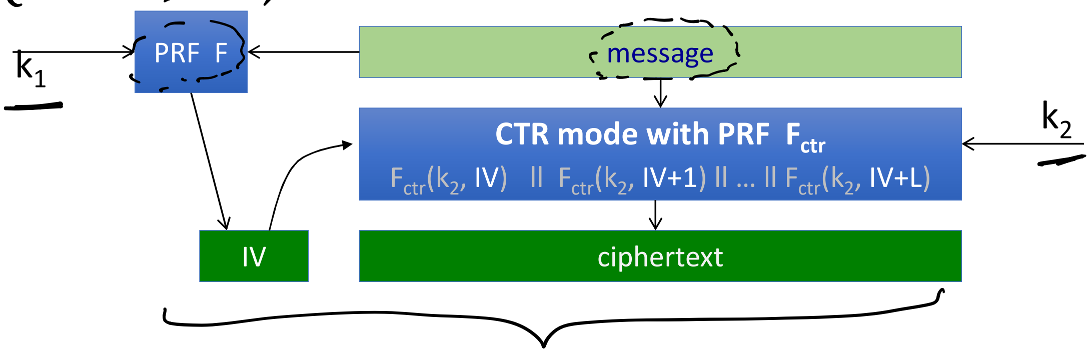
Goal: det. CPA security and ciphertext integrity

$\Rightarrow$ **DAE: deterministic authenticated encryption** = det. enc. + ciphertext integrity

Consider a SIV special case: SIV-CTR

SIV where cipher is counter mode with rand. IV

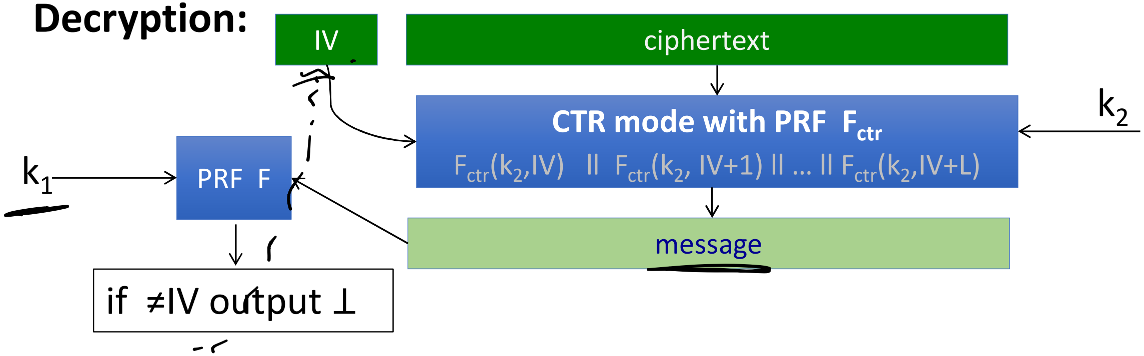
Enc(k_1, k_2, m)



IV' || ciphertext'

Deterministic Authenticated Encryption

Decryption:



Thm: If F is a secure PRF and CTR from F_{ctr} is CPA-secure then SIV-CTR from (F, F_{ctr}) provides DAE

Given $\boxed{IV' \,\|\, \text{ciphertext}'}$ decryption first computes message'. Apply $F(k_1, \text{message}')$ & check IV'!

Construction 2: Use a PRP

Let (E, D) be a secure PRP. E: $\underline{K} \times \underline{X} \longrightarrow \underline{X}$

<u>Thm</u>: (E,D) is sem. sec. under det. CPA .

Proof sketch: let $f: X \longrightarrow X$ be a truly random invertible func.

in EXP(0) adv. sees: $\mathbf{f(m_{1,0}), \ldots, f(m_{q,0})}$

in EXP(1) adv. sees: $\mathbf{f(m_{1,1}), \ldots, f(m_{q,1})}$

q random values in X

Using AES: Det. CPA secure encryption for 16 byte messages.

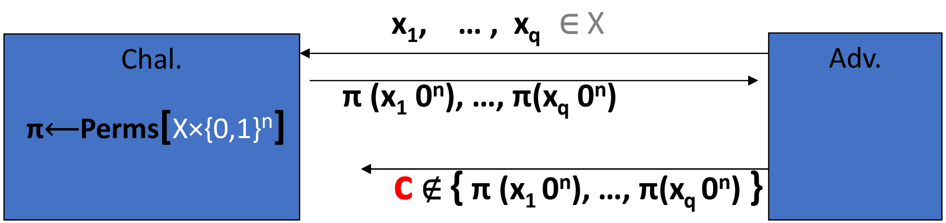
Longer messages?? Need PRPs on larger msg spaces…

PRP-based Deterministic Authenticated Encryption

Let (E, D) be a secure PRP. E: K × (X×{0,1}^{n}) ⟶ X×{0,1}^{n}

Thm: $1/2^n$ is negligible ⇒ PRP-based enc. provides DAE

Proof sketch: suffices to prove ciphertext integrity

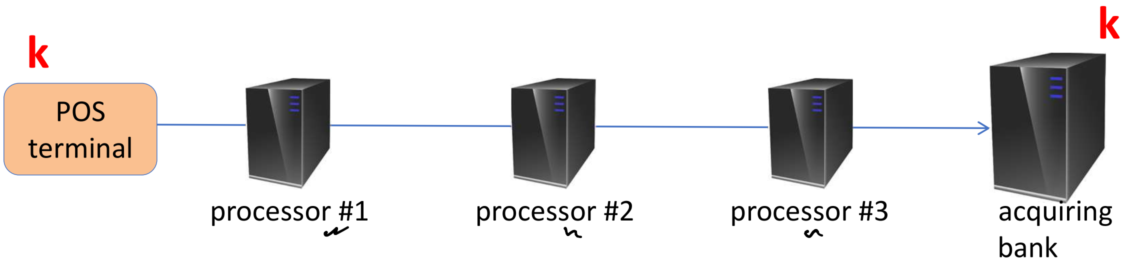


But then $\Pr[\ LSB_n(\ \pi^{-1}(c)\ ) = 0^n\ ] \leq 1/2^n$

Format-Preserving Encryption

Encrypting Credit Card Numbers

Credit card format: **bbbb bbnn nnnn nnnc** (≈ 42 bits)



Goal: end-to-end encryption

Intermediate processors expect to see a credit card number

⇒ encrypted credit card should look like a credit card

Format Preserving Encryption

10^{16}

Given $0 < s \leq 2^n$, build a PRP on $\{0,\ldots,s\text{-}1\}$

from a secure PRF $\mathbf{F: K \times \{0,1\}^n \longrightarrow \{0,1\}^n}$ (e.g. AES)

Then to encrypt a credit card number: (s = total # credit cards)

1. map given CC# to $\{0,\ldots,s\text{-}1\}$
2. apply PRP to get an output in $\{0,\ldots,s\text{-}1\}$
3. map output back a to CC#

PRF PRP

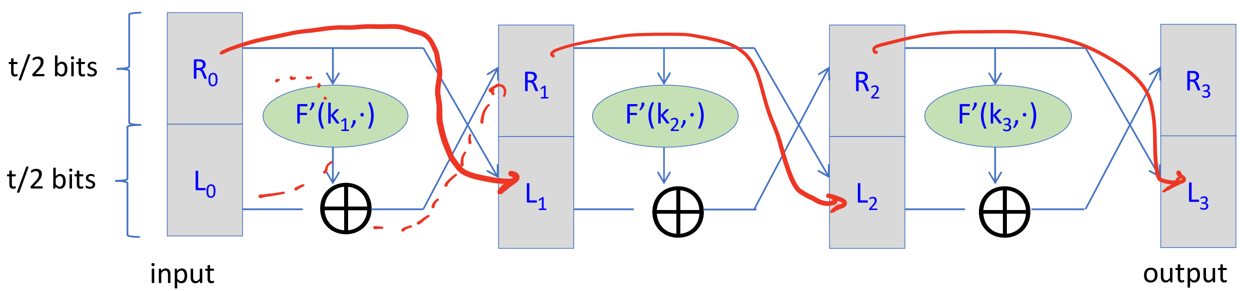
Step 1: From $\{0,1\}^n$ to $\{0,1\}^t$

$t = \lceil \log_2 s \rceil$

Want PRP on $\{0,\ldots,s\text{-}1\}$. Let t be such that $2^{t-1} < s \le 2^t$.

10^{16}

Method: Feistel with $F'\colon K \times \{0,1\}^{t/2} \longrightarrow \{0,1\}^{t/2}$ (truncate F) AES



(better to use 7 rounds a la Patarin, Crypto'03)

(uninvertible) PRF → (invertible) PRP.

from $\{0,1\}^t \rightarrow \{0,1\}^t$

$$2^t \geq s > 2^{t-1}$$

$10^{16}-1$

Step 2: From $\{0,1\}^t$ to $\{0, \ldots, s-1\}$

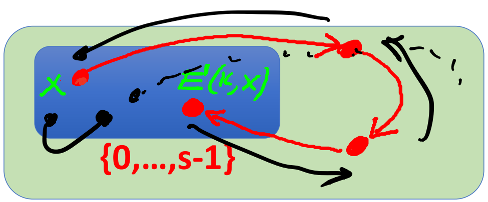
s may not be a power of 2.

Given PRP **(E,D): K × $\{0,1\}^t \longrightarrow \{0,1\}^t$**

we build **(E',D'): K × $\{0,\ldots,s-1\} \longrightarrow \{0,\ldots,s-1\}$**

E'(k, x): on input $x \in \{0,\ldots,s-1\}$ do:

$y \longleftarrow x$; do { $y \longleftarrow E(k, y)$ } until $y \in \{0,\ldots,s-1\}$; output y



$\{0,1\}^t$

Expected # iterations: 2

$$x \longrightarrow F(k,x) \longrightarrow F(k,F(k,x)) \longrightarrow F(k,F(k,F(k,x)))$$

(oops! >s) (oops! >s) <s

Security

Step 2 is tight: For all A, there exists B: $PRP_{adv}[A,E] = PRP_{adv}[B,E']$

Intuition: For all sets $Y \subseteq X$, applying the transformation to a
random perm. $\pi: X \longrightarrow X$
gives a random perm. $\pi': Y \longrightarrow Y$

Step 1: same security as Feistel construction

note: no integrity

Searchable Encryption.

Functional Encryption. $ct + fsk \longrightarrow Dec(fsk, ct)$
$\downarrow$
$f(pt)$

Number Theory

Public Key Encryption

Notation

From here on:

- N denotes a positive integer.
- p denote a prime.

Notation: $\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$

Can do addition and multiplication modulo N

$\forall a, b, \quad (a+b) \bmod N \in \mathbb{Z}_N$

Modular arithmetic

Examples: let $N = 12$

$$9 + 8 = 5 \quad \text{in } \mathbb{Z}_{12}$$

$$5 \times 7 = 11 \quad \text{in } \mathbb{Z}_{12}$$

$$5 - 7 = 10 \quad \text{in } \mathbb{Z}_{12}$$

$-2 \bmod 12 = 10$

Arithmetic in $\mathbb{Z}_N$ works as you expect, e.g $x \cdot (y+z) = x \cdot y + x \cdot z$ in $\mathbb{Z}_N$

Greatest common divisor

Def: For ints. x,y: **gcd(x, y)** is the greatest common divisor of x,y

Example: gcd(12, 18) = 6

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

$$a \cdot x + b \cdot y = \gcd(x,y) \quad \text{mod } N.$$

a,b can be found efficiently using the extended Euclid alg.

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

Modular inversion

$\frac{1}{2}$

Over the rationals, inverse of 2 is ½ . What about $\mathbb{Z}_N$?

Def: The **inverse** of x in $\mathbb{Z}_N$ is an element y in $\mathbb{Z}_N$ s.t. $x \cdot y = 1$ in $\mathbb{Z}_N$

y is denoted $x^{-1} \pmod N$

Example: let N be an odd integer. The inverse of 2 in $\mathbb{Z}_N$ is $\frac{N+1}{2}$.

Why?

$$2 \cdot \left(\frac{N+1}{2}\right) \bmod N = (N+1) \bmod N$$

$$= 1 \bmod N$$

50 mod 6 = 2.

a mod N =

Divide a/N

take the remainder.

Modular inversion

Which elements have an inverse in $\mathbb{Z}_N$?

Lemma: x in $\mathbb{Z}_N$ has an inverse if and only if gcd(x,N) = 1

Proof:

$\gcd(x,N)=1 \overset{\text{Euclid}}{\Rightarrow} \exists\, a,b:\ \underbrace{a\cdot x + b\cdot N = 1}_{\text{mod } N \text{ on both sides}} \Longrightarrow a\cdot x = 1 \text{ in } \mathbb{Z}_N$

$\gcd(x,N) > 1 \Rightarrow \forall a:\ \gcd(a\cdot x, N) > 1 \Rightarrow a\cdot x \neq 1 \text{ in } \mathbb{Z}_N$

$\gcd(x,N) = 2 \Longrightarrow \forall a:\ a.x \text{ is even} \Longrightarrow \overset{\text{even}}{a.x} \neq \overset{\text{odd}}{b.N+1}$

$\Rightarrow x$ is not invertible mod N.

More notation

Def: $\mathbb{Z}_N^*$ = (set of invertible elements in $\mathbb{Z}_N$) =

= { x∈ $\mathbb{Z}_N$: gcd(x,N) = 1 }

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$
$= \{x : GCD(x,5) = 1\}$

Examples:

1. for prime p, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \underbrace{\{1, 2, \ldots, p-1\}}_{\text{all are invertible}}$

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

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

Solving modular linear equations

Solve: $\mathbf{a \cdot x + b = \overset{5}{0}}$ **in** $\mathbb{Z}_N$

$\Rightarrow a \cdot x = -b \Rightarrow x = -b \cdot a^{-1} = a^{-1}(-b)$

Solution: $\mathbf{x = -b \cdot a^{-1}}$ **in** $\mathbb{Z}_N$

Find a^{-1} in $\mathbb{Z}_N$ using extended Euclid. Run time: $O(\log^2 N)$

What about modular quadratic equations? (next time..)