BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Low e Attacks on RSA

Scenario

Scenario

1. Zelda is sending messages to Alice using $N_a = 377$, $e = 3$.

Scenario

1. Zelda is sending messages to Alice using $N_a = 377$, $e = 3$.
2. Zelda is sending messages to Bob using $N_b = 391$, $e = 3$.

Scenario

1. Zelda is sending messages to Alice using $N_a = 377$, $e = 3$.
2. Zelda is sending messages to Bob using $N_b = 391$, $e = 3$.

e is low. That will make the system crackable if ...

Scenario

1. Zelda is sending messages to Alice using $N_a = 377$, $e = 3$.
2. Zelda is sending messages to Bob using $N_b = 391$, $e = 3$.

e is low. That will make the system crackable if ...
Zelda sends *same* m to all three. **Note** $m < 377$. Zelda does this:

Scenario

1. Zelda is sending messages to Alice using $N_a = 377$, $e = 3$.
2. Zelda is sending messages to Bob using $N_b = 391$, $e = 3$.

e is low. That will make the system crackable if ...
Zelda sends *same* m to all three. **Note** $m < 377$. Zelda does this:

1. Zelda sends Alice 359. So $m^3 \equiv 359 \pmod{377}$.

Scenario

1. Zelda is sending messages to Alice using $N_a = 377$, $e = 3$.
2. Zelda is sending messages to Bob using $N_b = 391$, $e = 3$.

e is low. That will make the system crackable if ...
Zelda sends *same* m to all three. **Note** $m < 377$. Zelda does this:

1. Zelda sends Alice 359. So $m^3 \equiv 359 \pmod{377}$.
2. Zelda sends Bob 247. So $m^3 \equiv 247 \pmod{391}$.

Scenario

1. Zelda is sending messages to Alice using $N_a = 377$, $e = 3$.
2. Zelda is sending messages to Bob using $N_b = 391$, $e = 3$.

e is low. That will make the system crackable if ...
Zelda sends *same* m to all three. **Note** $m < 377$. Zelda does this:

1. Zelda sends Alice 359. So $m^3 \equiv 359 \pmod{377}$.
2. Zelda sends Bob 247. So $m^3 \equiv 247 \pmod{391}$.

Eve can use this information to find m.

Scenario

1. Zelda is sending messages to Alice using $N_a = 377$, $e = 3$.
2. Zelda is sending messages to Bob using $N_b = 391$, $e = 3$.

e is low. That will make the system crackable if ...
Zelda sends *same* m to all three. **Note** $m < 377$. Zelda does this:

1. Zelda sends Alice 359. So $m^3 \equiv 359 \pmod{377}$.
2. Zelda sends Bob 247. So $m^3 \equiv 247 \pmod{391}$.

Eve can use this information to find m.
We will develop the math and the attack. Called **a low-e attack**.

Chinese Remainder Theorem: Example

Find x such that:
$x \equiv 17 \pmod{31}$
$x \equiv 20 \pmod{37}$

Chinese Remainder Theorem: Example

Find x such that:

$x \equiv 17 \pmod{31}$

$x \equiv 20 \pmod{37}$

a) The inverse of 31 mod 37 is **6**.

b) The inverse of 37 mod 31 is **26**.

Chinese Remainder Theorem: Example

Find x such that:
$x \equiv 17 \pmod{31}$
$x \equiv 20 \pmod{37}$
a) The inverse of 31 mod 37 is **6**.
b) The inverse of 37 mod 31 is **26**.

$$x = 20 \times \mathbf{6} \times 31 + 17 \times \mathbf{26} \times 37 = 20,074$$

$x \pmod{31}$: 1st=0. 2nd$= 17 \times 26 \times 26^{-1} \equiv 17$. Sum=17.

Chinese Remainder Theorem: Example

Find x such that:
$x \equiv 17 \pmod{31}$
$x \equiv 20 \pmod{37}$
a) The inverse of 31 mod 37 is **6**.
b) The inverse of 37 mod 31 is **26**.

$$x = 20 \times \mathbf{6} \times 31 + 17 \times \mathbf{26} \times 37 = 20,074$$

$x \pmod{31}$: 1st=0. 2nd$= 17 \times 26 \times 26^{-1} \equiv 17$. Sum=17.
$x \pmod{37}$: 1st$= 20 \times 31^{-1} \times 31 \equiv 20$. 2nd=0. Sum=20.

Chinese Remainder Theorem: Example

Find x such that:
$x \equiv 17 \pmod{31}$
$x \equiv 20 \pmod{37}$
a) The inverse of 31 mod 37 is **6**.
b) The inverse of 37 mod 31 is **26**.

$$x = 20 \times \mathbf{6} \times 31 + 17 \times \mathbf{26} \times 37 = 20{,}074$$

$x \pmod{31}$: 1st=0. 2nd$= 17 \times 26 \times 26^{-1} \equiv 17$. Sum=17.
$x \pmod{37}$: 1st$= 20 \times 31^{-1} \times 31 \equiv 20$. 2nd=0. Sum=20.
So $x = 20{,}074$ is an answer.

Chinese Remainder Theorem: Example (cont)

Find x such that:

$$x \equiv 17 \pmod{31} \qquad \& \qquad x \equiv 20 \pmod{37}$$

Chinese Remainder Theorem: Example (cont)

Find x such that:

$$x \equiv 17 \pmod{31} \qquad \& \qquad x \equiv 20 \pmod{37}$$

From last slide: So $x = 20,074$ works. Smaller x?

Chinese Remainder Theorem: Example (cont)

Find x such that:

$$x \equiv 17 \pmod{31} \qquad \& \qquad x \equiv 20 \pmod{37}$$

From last slide: So $x = 20,074$ works. Smaller x?
We only care about $x \pmod{31}$ and $x \pmod{37}$.

Chinese Remainder Theorem: Example (cont)

Find x such that:

$$x \equiv 17 \pmod{31} \qquad \& \qquad x \equiv 20 \pmod{37}$$

From last slide: So $x = 20,074$ works. Smaller x?
We only care about $x \pmod{31}$ and $x \pmod{37}$.
So only care about $x \pmod{31 \times 37}$

Chinese Remainder Theorem: Example (cont)

Find x such that:

$$x \equiv 17 \pmod{31} \qquad \& \qquad x \equiv 20 \pmod{37}$$

From last slide: So $x = 20,074$ works. Smaller x?
We only care about $x \pmod{31}$ and $x \pmod{37}$.
So only care about $x \pmod{31 \times 37}$

If x works then $x \bmod 31 \times 37$ works. So just need

$$20,074 \equiv 575 \pmod{31 \times 37}$$

Chinese Remainder Theorem: Example (cont)

Find x such that:

$$x \equiv 17 \pmod{31} \qquad \& \qquad x \equiv 20 \pmod{37}$$

From last slide: So $x = 20,074$ works. Smaller x?
We only care about $x \pmod{31}$ and $x \pmod{37}$.
So only care about $x \pmod{31 \times 37}$

If x works then $x \bmod 31 \times 37$ works. So just need

$$20,074 \equiv 575 \pmod{31 \times 37}$$

Upshot: Can take $x = 575$.

What if $x = m^2$ is a Square?

Find m such that:

$$m^2 \equiv 8 \pmod{17} \qquad \& \qquad m^2 \equiv 25 \pmod{37}$$

a) The inverse of 17 mod 37 is 24.
b) The inverse of 37 mod 17 is 6.

What if $x = m^2$ is a Square?

Find m such that:

$$m^2 \equiv 8 \pmod{17} \qquad \& \qquad m^2 \equiv 25 \pmod{37}$$

a) The inverse of 17 mod 37 is 24.
b) The inverse of 37 mod 17 is 6.

$$m^2 = 8 \times 37 \times 6 + 25 \times 17 \times 24 = 11976$$

$11976 \equiv 25 \pmod{17 \times 37}$.

What if $x = m^2$ is a Square?

Find m such that:

$$m^2 \equiv 8 \pmod{17} \qquad \& \qquad m^2 \equiv 25 \pmod{37}$$

a) The inverse of 17 mod 37 is 24.
b) The inverse of 37 mod 17 is 6.

$$m^2 = 8 \times 37 \times 6 + 25 \times 17 \times 24 = 11976$$

$11976 \equiv 25 \pmod{17 \times 37}$.
OH, $m^2 \equiv 25$. This is a square in $\mathbb{N}$. So $m = 5$.

What if $x = m^3$?

Find m such that:

$$m^3 \equiv 12 \pmod{17} \qquad \& \qquad m^3 \equiv 16 \pmod{37}$$

What if $x = m^3$?

Find m such that:

$$m^3 \equiv 12 \pmod{17} \qquad \& \qquad m^3 \equiv 16 \pmod{37}$$

a) The inverse of 17 mod 37 is 24.
b) The inverse of 37 mod 17 is 6.

What if $x = m^3$?

Find m such that:

$$m^3 \equiv 12 \pmod{17} \qquad \& \qquad m^3 \equiv 16 \pmod{37}$$

a) The inverse of 17 mod 37 is 24.
b) The inverse of 37 mod 17 is 6.

$$m^3 = 12 \times 37 \times 6 + 16 \times 17 \times 24 = 9192$$

$9192 \equiv 386 \pmod{17 \times 37}$.

What if $x = m^3$?

Find m such that:

$$m^3 \equiv 12 \pmod{17} \qquad \& \qquad m^3 \equiv 16 \pmod{37}$$

a) The inverse of 17 mod 37 is 24.
b) The inverse of 37 mod 17 is 6.

$$m^3 = 12 \times 37 \times 6 + 16 \times 17 \times 24 = 9192$$

$9192 \equiv 386 \pmod{17 \times 37}$.
OH, $m^3 \equiv 386$. This is NOT a cube :-(What was different?

Squares and Cubes

Find m such that:

$$m^2 \equiv 8 \pmod{17} \qquad \& \qquad m^2 \equiv 25 \pmod{37}$$

The message m is < 17 and < 37. So
$m^2 < 17 \times 17$. So $m^2 = m^2 \pmod{17 \times 37}$ (no reduce).

Squares and Cubes

Find m such that:

$$m^2 \equiv 8 \pmod{17} \qquad \& \qquad m^2 \equiv 25 \pmod{37}$$

The message m is < 17 and < 37. So
$m^2 < 17 \times 17$. So $m^2 = m^2 \pmod{17 \times 37}$ (no reduce).

Find m such that:

$$m^3 \equiv 12 \pmod{17} \qquad \& \qquad m^3 \equiv 16 \pmod{37}$$

Squares and Cubes

Find m such that:

$$m^2 \equiv 8 \pmod{17} \qquad \& \qquad m^2 \equiv 25 \pmod{37}$$

The message m is < 17 and < 37. So $m^2 < 17 \times 17$. So $m^2 = m^2 \pmod{17 \times 37}$ (no reduce).

Find m such that:

$$m^3 \equiv 12 \pmod{17} \qquad \& \qquad m^3 \equiv 16 \pmod{37}$$

The message m is < 17 and < 37, so $m^3 < 17^3 = 4913$. So $m^3 \pmod{17 \times 37}$ CAN reduce. So DO NOT get that

$$m^3 \pmod{17 \times 37} = m^3$$

Squares and Cubes

Find m such that:

$$m^2 \equiv 8 \pmod{17} \qquad \& \qquad m^2 \equiv 25 \pmod{37}$$

The message m is < 17 and < 37. So
$m^2 < 17 \times 17$. So $m^2 = m^2 \pmod{17 \times 37}$ (no reduce).

Find m such that:

$$m^3 \equiv 12 \pmod{17} \qquad \& \qquad m^3 \equiv 16 \pmod{37}$$

The message m is < 17 and < 37, so $m^3 < 17^3 = 4913$.
So $m^3 \pmod{17 \times 37}$ CAN reduce. So DO NOT get that

$$m^3 \pmod{17 \times 37} = m^3$$

We return to this point in a few slides.

Back to our Example

$$m^3 \equiv 359 \pmod{377}$$
$$m^3 \equiv 247 \pmod{391}$$

Back to our Example

$$m^3 \equiv 359 \pmod{377}$$
$$m^3 \equiv 247 \pmod{391}$$
$$m^3 =$$
$$359 \times 391 \times (391^{-1} \pmod{377}) + 247 \times 377 \times (377^{-1} \pmod{391})$$

Back to our Example

$m^3 \equiv 359 \pmod{377}$
$m^3 \equiv 247 \pmod{391}$
$m^3 =$
$359 \times 391 \times (391^{-1} \pmod{377}) + 247 \times 377 \times (377^{-1} \pmod{391})$
$391^{-1} \pmod{377} = 27.$

Back to our Example

$m^3 \equiv 359 \pmod{377}$
$m^3 \equiv 247 \pmod{391}$
$m^3 =$
$359 \times 391 \times (391^{-1} \pmod{377}) + 247 \times 377 \times (377^{-1} \pmod{391})$
$391^{-1} \pmod{377} = 27.$
$377^{-1} \pmod{391} = 363.$

Back to our Example

$m^3 \equiv 359 \pmod{377}$
$m^3 \equiv 247 \pmod{391}$
$m^3 =$
$359 \times 391 \times (391^{-1} \pmod{377}) + 247 \times 377 \times (377^{-1} \pmod{391})$
$391^{-1} \pmod{377} = 27.$
$377^{-1} \pmod{391} = 363.$
$m^3 = 359 \times 391 \times 27 + 247 \times 377 \times 363 \equiv 3375 \pmod{377 \times 391}.$

Back to our Example

$m^3 \equiv 359 \pmod{377}$
$m^3 \equiv 247 \pmod{391}$
$m^3 =$
$359 \times 391 \times (391^{-1} \pmod{377}) + 247 \times 377 \times (377^{-1} \pmod{391})$
$391^{-1} \pmod{377} = 27.$
$377^{-1} \pmod{391} = 363.$
$m^3 = 359 \times 391 \times 27 + 247 \times 377 \times 363 \equiv 3375 \pmod{377 \times 391}.$
Does 3375 have an INTEGER cube root?

Back to our Example

$m^3 \equiv 359 \pmod{377}$
$m^3 \equiv 247 \pmod{391}$
$m^3 =$
$359 \times 391 \times (391^{-1} \pmod{377}) + 247 \times 377 \times (377^{-1} \pmod{391})$
$391^{-1} \pmod{377} = 27.$
$377^{-1} \pmod{391} = 363.$
$m^3 = 359 \times 391 \times 27 + 247 \times 377 \times 363 \equiv 3375 \pmod{377 \times 391}.$
Does 3375 have an INTEGER cube root? YES: 15.

Back to our Example

$m^3 \equiv 359 \pmod{377}$
$m^3 \equiv 247 \pmod{391}$
$m^3 =$
$359 \times 391 \times (391^{-1} \pmod{377}) + 247 \times 377 \times (377^{-1} \pmod{391})$
$391^{-1} \pmod{377} = 27.$
$377^{-1} \pmod{391} = 363.$
$m^3 = 359 \times 391 \times 27 + 247 \times 377 \times 363 \equiv 3375 \pmod{377 \times 391}.$
Does 3375 have an INTEGER cube root? YES: 15. Can verify
$m = 15$:

Back to our Example

$m^3 \equiv 359 \pmod{377}$
$m^3 \equiv 247 \pmod{391}$
$m^3 =$
$359 \times 391 \times (391^{-1} \pmod{377}) + 247 \times 377 \times (377^{-1} \pmod{391})$
$391^{-1} \pmod{377} = 27.$
$377^{-1} \pmod{391} = 363.$
$m^3 = 359 \times 391 \times 27 + 247 \times 377 \times 363 \equiv 3375 \pmod{377 \times 391}.$
Does 3375 have an INTEGER cube root? YES: 15. Can verify
$m = 15$:
$15^3 \equiv 359 \pmod{377}$

Back to our Example

$m^3 \equiv 359 \pmod{377}$
$m^3 \equiv 247 \pmod{391}$
$m^3 =$
$359 \times 391 \times (391^{-1} \pmod{377}) + 247 \times 377 \times (377^{-1} \pmod{391})$
$391^{-1} \pmod{377} = 27.$
$377^{-1} \pmod{391} = 363.$
$m^3 = 359 \times 391 \times 27 + 247 \times 377 \times 363 \equiv 3375 \pmod{377 \times 391}.$
Does 3375 have an INTEGER cube root? YES: 15. Can verify
$m = 15$:
$15^3 \equiv 359 \pmod{377}$
$15^3 \equiv 247 \pmod{391}$

Chinese Remainder Theorem: N_1, N_2 Case

Chinese Remainder Theorem: N_1, N_2 Case

1. Input a, b, N_1, N_2, with N_1, N_2, rel prime. Want $0 \le x < N_1 N_2$:
   $x \equiv a \pmod{N_1}$
   $x \equiv b \pmod{N_2}$

Chinese Remainder Theorem: N_1, N_2 Case

1. Input a, b, N_1, N_2, with N_1, N_2, rel prime. Want $0 \le x < N_1 N_2$:
   $x \equiv a \pmod{N_1}$
   $x \equiv b \pmod{N_2}$
2. Find the inverse of N_1 mod N_2 and denote this N_1^{-1}.

Chinese Remainder Theorem: N_1, N_2 Case

1. Input a, b, N_1, N_2, with N_1, N_2, rel prime. Want
   $0 \le x < N_1 N_2$:
   $x \equiv a \pmod{N_1}$
   $x \equiv b \pmod{N_2}$
2. Find the inverse of N_1 mod N_2 and denote this N_1^{-1}.
3. Find the inverse of N_2 mod N_1 and denote this N_2^{-1}.

Chinese Remainder Theorem: N_1, N_2 Case

1. Input a, b, N_1, N_2, with N_1, N_2, rel prime. Want
   $0 \le x < N_1 N_2$:
   $x \equiv a \pmod{N_1}$
   $x \equiv b \pmod{N_2}$
2. Find the inverse of N_1 mod N_2 and denote this N_1^{-1}.
3. Find the inverse of N_2 mod N_1 and denote this N_2^{-1}.
4. $y = bN_1^{-1}N_1 + aN_2^{-1}N_2$

   Mod N_1: 1st term is 0, 2nd term is a. So $y \equiv a \pmod{N_1}$.

   Mod N_2: 2nd term is 0, 1st term is b. So $y \equiv b \pmod{N_2}$.

Chinese Remainder Theorem: N_1, N_2 Case

1. Input a, b, N_1, N_2, with N_1, N_2, rel prime. Want
   $0 \le x < N_1 N_2$:
   $x \equiv a \pmod{N_1}$
   $x \equiv b \pmod{N_2}$
2. Find the inverse of N_1 mod N_2 and denote this N_1^{-1}.
3. Find the inverse of N_2 mod N_1 and denote this N_2^{-1}.
4. $y = bN_1^{-1}N_1 + aN_2^{-1}N_2$

   Mod N_1: 1st term is 0, 2nd term is a. So $y \equiv a \pmod{N_1}$.

   Mod N_2: 2nd term is 0, 1st term is b. So $y \equiv b \pmod{N_2}$.
5. $x \equiv y \pmod{N_1 N_2}$. (Convention that $0 \le x < N_1 N_2$)

The e Theorem, N_1, N_2 case

Theorem: Assume N_1, N_2 are rel prime, $e, m \in \mathbb{N}$. Let $0 \le x < N_1 N_2$ be the number from CRT such that
$x \equiv m^e \pmod{N_1}$
$x \equiv m^e \pmod{N_2}$
Then $x \equiv m^e \pmod{N_1 N_2}$. **IF** $m^e < N_1 N_2$ **then** $x = m^e$**.**

The e Theorem, N_1, N_2 case

Theorem: Assume N_1, N_2 are rel prime, $e, m \in \mathbb{N}$. Let $0 \le x < N_1 N_2$ be the number from CRT such that
$x \equiv m^e \pmod{N_1}$
$x \equiv m^e \pmod{N_2}$
Then $x \equiv m^e \pmod{N_1 N_2}$. **IF $m^e < N_1 N_2$ then $x = m^e$.**

Proof: There exists k_1, k_2 such that
$x = m^e + k_1 N_1$ $\quad$ $k_1 \in \mathbb{Z}$, (Could be negative)
$x = m^e + k_2 N_2$ $\quad$ $k_2 \in \mathbb{Z}$, (Could be negative)

The e Theorem, N_1, N_2 case

Theorem: Assume N_1, N_2 are rel prime, $e, m \in \mathbb{N}$. Let
$0 \le x < N_1 N_2$ be the number from CRT such that
$x \equiv m^e \pmod{N_1}$
$x \equiv m^e \pmod{N_2}$
Then $x \equiv m^e \pmod{N_1 N_2}$. **IF $m^e < N_1 N_2$ then $x = m^e$.**

Proof: There exists k_1, k_2 such that
$x = m^e + k_1 N_1 \qquad k_1 \in \mathbb{Z}$, (Could be negative)
$x = m^e + k_2 N_2 \qquad k_2 \in \mathbb{Z}$, (Could be negative)

$k_1 N_1 = k_2 N_2$. Since N_1, N_2 rel prime, N_1 divides k_2, so $k_2 = kN_1$.

The e Theorem, N_1, N_2 case

Theorem: Assume N_1, N_2 are rel prime, $e, m \in \mathbb{N}$. Let $0 \le x < N_1 N_2$ be the number from CRT such that
$x \equiv m^e \pmod{N_1}$
$x \equiv m^e \pmod{N_2}$
Then $x \equiv m^e \pmod{N_1 N_2}$. **IF** $m^e < N_1 N_2$ **then** $x = m^e$**.**

Proof: There exists k_1, k_2 such that
$x = m^e + k_1 N_1 \qquad k_1 \in \mathbb{Z}$, (Could be negative)
$x = m^e + k_2 N_2 \qquad k_2 \in \mathbb{Z}$, (Could be negative)

$k_1 N_1 = k_2 N_2$. Since N_1, N_2 rel prime, N_1 divides k_2, so $k_2 = kN_1$.

$x = m^e + kN_1 N_2$. Hence $x \equiv m^e \pmod{N_1 N_2}$.
If $m^e < N_1 N_2$ then since $0 \le x < N_1 N_2$ & $x \equiv m^e$, $x = m^e$.

Using CRT to find m: N_1, N_2 Case

Theorem: Assume N_1, N_2 are rel prime, $e, m \in \mathbb{N}$, $e = 2$, and $m < N_1, N_2$. Assume you are given, x_1, x_2 such that

$m^2 \equiv x_1 \pmod{N_1}$

$m^2 \equiv x_2 \pmod{N_2}$.

(you are NOT given m). Then you can find m.

Using CRT to find m: N_1, N_2 Case

Theorem: Assume N_1, N_2 are rel prime, $e, m \in \mathbb{N}$, $e = 2$, and $m < N_1, N_2$. Assume you are given,x_1, x_2 such that
$m^2 \equiv x_1 \pmod{N_1}$
$m^2 \equiv x_2 \pmod{N_2}$.
(you are NOT given m). Then you can find m.
Proof: Use CRT to find x such that

$$\begin{aligned} x &\equiv x_1 \pmod{N_1} \\ x &\equiv x_2 \pmod{N_2} \end{aligned}$$

and $0 \le x < N_1 N_2$.
Since $m < N_1, N_2$, $m^2 < N_1 N_2$.
Hence x is a square root in $\mathbb{N}$. Take the square root to find m.
End of Proof
Note In $e = 2$, $m < N_1 N_2$ case can crack RSA without factoring!

Generalize this Attack

We cracked RSA if $e = 2$ and $M < N_1 N_2$.

Generalize this Attack

We cracked RSA if $e = 2$ and $M < N_1 N_2$.
We will generalize:

Generalize this Attack

We cracked RSA if $e = 2$ and $M < N_1 N_2$.
We will generalize:

1. We present general Chinese Remainder Remainder.

Generalize this Attack

We cracked RSA if $e = 2$ and $M < N_1 N_2$.
We will generalize:

1. We present general Chinese Remainder Remainder.
2. We present general e-theorem.

Generalize this Attack

We cracked RSA if $e = 2$ and $M < N_1 N_2$.
We will generalize:

1. We present general Chinese Remainder Remainder.
2. We present general e-theorem.
3. We present full low-e attack.

The Chinese Remainder Theorem: $N_1, \ldots, N_L$ Case

Theorem: If $N_1, \ldots, N_L$ are rel prime, $x_1, \ldots, x_L$ are anything, then there exists x with $0 \le x < N_1 \cdots N_L$ such that

$$\begin{aligned} x &\equiv x_1 \pmod{N_1} \\ x &\equiv x_2 \pmod{N_2} \\ &\vdots \\ x &\equiv x_L \pmod{N_L} \end{aligned}$$

Proof: Omitted.

Notation: CRT is Chinese Remainder Theorem.

The e Theorem, $N_1, \ldots, N_L$ Case

Theorem: Assume $N_1, \ldots, N_L$ are rel prime, $e, m \in \mathbb{N}$.

$$\begin{aligned} x &\equiv m^e \pmod{N_1} \\ &\vdots \qquad\qquad \vdots \\ x &\equiv m^e \pmod{N_L} \end{aligned}$$

Then $x \equiv m^e \pmod{N_1 \cdots N_L}$. **If $m^e < N_1 \cdots N_L$ then $x = m^e$.**
Proof: Omitted.

Using CRT to find m

Theorem: Assume $N_1, \ldots, N_L$ are rel prime, $e, m \in \mathbb{N}$, $e \le L$, and for all i, $m < N_i$. Assume you are given, for all i, x_i such that $m^e \equiv x_i \pmod{N_i}$ (you are NOT given m). Then you can find m.

Using CRT to find m

Theorem: Assume $N_1, \ldots, N_L$ are rel prime, $e, m \in \mathbb{N}$, $e \le L$, and for all i, $m < N_i$. Assume you are given, for all i, x_i such that $m^e \equiv x_i \pmod{N_i}$ (you are NOT given m). Then you can find m.
Proof: Use CRT to find x such that

$$\begin{aligned} x &\equiv x_1 \pmod{N_1} \\ &\vdots \\ x &\equiv x_L \pmod{N_L} \end{aligned}$$

and $0 \le x < N_1 \cdots N_L$.
Since $m < N_i$ and $e \le L$, $m^e < N_1 \cdots N_L$.
Hence x is an eth power in $\mathbb{N}$. Take the eth root to find m.
End of Proof

Low Exponent Attack: Example

Low Exponent Attack: Example

1) $N_a = 377$, $N_b = 391$, $N_c = 589$. For Alice, Bob, Carol.

Low Exponent Attack: Example

1) $N_a = 377$, $N_b = 391$, $N_c = 589$. For Alice, Bob, Carol.
2) $e = 3$.

Low Exponent Attack: Example

1) $N_a = 377$, $N_b = 391$, $N_c = 589$. For Alice, Bob, Carol.
2) $e = 3$.
3) Zelda sends m to all three. Eve will find m. **Note** $m < 377$.

1. Zelda sends Alice 330. So $m^3 \equiv 330 \pmod{377}$.
2. Zelda sends Bob 34. So $m^3 \equiv 34 \pmod{391}$.
3. Zelda sends Carol 419. So $m^3 \equiv 419 \pmod{589}$.

Low Exponent Attack: Example

1) $N_a = 377$, $N_b = 391$, $N_c = 589$. For Alice, Bob, Carol.
2) $e = 3$.
3) Zelda sends m to all three. Eve will find m. **Note** $m < 377$.

1. Zelda sends Alice 330. So $m^3 \equiv 330 \pmod{377}$.
2. Zelda sends Bob 34. So $m^3 \equiv 34 \pmod{391}$.
3. Zelda sends Carol 419. So $m^3 \equiv 419 \pmod{589}$.

Eve sees all of this. Eve uses CRT to find $0 \le x < 377 \times 391 \times 589$.

$x \equiv 330 \equiv m^3 \pmod{377}$

$x \equiv 34 \equiv m^3 \pmod{391}$

$x \equiv 419 \equiv m^3 \pmod{589}$

Low Exponent Attack: Example

1) $N_a = 377$, $N_b = 391$, $N_c = 589$. For Alice, Bob, Carol.
2) $e = 3$.
3) Zelda sends m to all three. Eve will find m. **Note** $m < 377$.

1. Zelda sends Alice 330. So $m^3 \equiv 330 \pmod{377}$.
2. Zelda sends Bob 34. So $m^3 \equiv 34 \pmod{391}$.
3. Zelda sends Carol 419. So $m^3 \equiv 419 \pmod{589}$.

Eve sees all of this. Eve uses CRT to find $0 \le x < 377 \times 391 \times 589$.
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$
Eve finds such a number: $x = 1,061,208$. (SEE NEXT SLIDE FOR HOW I GOT THAT)
By e-Theorem

$$1,061,208 \equiv m^3 \pmod{377 \times 391 \times 589}.$$

Since $1,061,208 < 377 \times 391 \times 589$, $1,061,208 = m^3$.

HOW I GOT 1,061,208: Part One

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$

HOW I GOT 1,061,208: Part One

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$
We want a term that:
Mod 377 gives 330, Mod 391 gives 0, Mod 589 gives 0.

$$330 \times 391 \times 589$$

is indeed 0 mod 391 and 0 mod 589. But it's NOT 330 mod 377.
So we need x such that $391 \times 589 \times x \equiv 1 \pmod{377}$.
$391 \times 589 \equiv 329 \pmod{377}$

HOW I GOT 1,061,208: Part One

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$
We want a term that:
Mod 377 gives 330, Mod 391 gives 0, Mod 589 gives 0.

$$330 \times 391 \times 589$$

is indeed 0 mod 391 and 0 mod 589. But it's NOT 330 mod 377.
So we need x such that $391 \times 589 \times x \equiv 1 \pmod{377}$.
$391 \times 589 \equiv 329 \pmod{377}$
So we need the inverse of 329 mod 377. That's 322. So the term we need is

$$330 \times 391 \times 589 \times 322 = 24471571740$$

For the next two terms, the next two slides.

HOW I GOT 1,061,208: Part Two

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$

HOW I GOT 1,061,208: Part Two

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$
We want a term that:
Mod 391 gives 34, Mod 377 gives 0, Mod 589 gives 0.

$$34 \times 377 \times 589$$

is indeed 0 mod 377 and 0 mod 589. But it's NOT 34 mod 391.

HOW I GOT 1,061,208: Part Two

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$
We want a term that:
Mod 391 gives 34, Mod 377 gives 0, Mod 589 gives 0.

$$34 \times 377 \times 589$$

is indeed 0 mod 377 and 0 mod 589. But it's NOT 34 mod 391.
So we need x such that $377 \times 589 \times x \equiv 1 \pmod{391}$.
$377 \times 589 \equiv 356 \pmod{391}$
So we need the inverse of 356 mod 391. That's 67. So the term we need is

$$34 \times 377 \times 589 \times 67 = 505836734$$

HOW I GOT 1,061,208: Part Two

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$
We want a term that:
Mod 391 gives 34, Mod 377 gives 0, Mod 589 gives 0.

$$34 \times 377 \times 589$$

is indeed 0 mod 377 and 0 mod 589. But it's NOT 34 mod 391.
So we need x such that $377 \times 589 \times x \equiv 1 \pmod{391}$.
$377 \times 589 \equiv 356 \pmod{391}$
So we need the inverse of 356 mod 391. That's 67. So the term we need is

$$34 \times 377 \times 589 \times 67 = 505836734$$

For the third term, the next slides.

HOW I GOT 1,061,208: Part Three

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$

HOW I GOT 1,061,208: Part Three

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$
We want a term that:
Mod 589 gives 419, Mod 377 gives 0, Mod 391 gives 0.

$$419 \times 377 \times 391$$

is indeed 0 mod 377 and 0 mod 391. But it's NOT 419 mod 589.

HOW I GOT 1,061,208: Part Three

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$
We want a term that:
Mod 589 gives 419, Mod 377 gives 0, Mod 391 gives 0.

$$419 \times 377 \times 391$$

is indeed 0 mod 377 and 0 mod 391. But it's NOT 419 mod 589.
So we need x such that $377 \times 391 \times x \equiv 1 \pmod{589}$.
$377 \times 391 \equiv 157 \pmod{589}$
So we need the inverse of 157 mod 589. That's 574
So the term we need is

$$419 \times 377 \times 391 \times 574 = 35452267942$$

HOW I GOT 1,061,208: Part Three

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$
We want a term that:
Mod 589 gives 419, Mod 377 gives 0, Mod 391 gives 0.

$$419 \times 377 \times 391$$

is indeed 0 mod 377 and 0 mod 391. But it's NOT 419 mod 589.
So we need x such that $377 \times 391 \times x \equiv 1 \pmod{589}$.
$377 \times 391 \equiv 157 \pmod{589}$
So we need the inverse of 157 mod 589. That's 574
So the term we need is

$$419 \times 377 \times 391 \times 574 = 35452267942$$

On the next slide we add up the terms!

HOW I GOT 1,061,208: The Finale!

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$

HOW I GOT 1,061,208: The Finale!

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$
We have deduced that it is the following sum

$$24471571740 + 505836734 + 35452267942 = 60429676416$$

HOW I GOT 1,061,208: The Finale!

We want an x such that
$x \equiv 330 \equiv m^3 \pmod{377}$
$x \equiv 34 \equiv m^3 \pmod{391}$
$x \equiv 419 \equiv m^3 \pmod{589}$
We have deduced that it is the following sum

$$24471571740 + 505836734 + 35452267942 = 60429676416$$

This number works. Now we take it mod $377 * 391 * 589$ to get

$$1,061,208$$

Low Exponent Attack: Example Continued

By e-Theorem

$$1,061,208 \equiv m^3 \pmod{377 \times 391 \times 589}.$$

Low Exponent Attack: Example Continued

By e-Theorem

$$1,061,208 \equiv m^3 \pmod{377 \times 391 \times 589}.$$

Most Important Fact Recall that $m < 377$. Hence note that:

$$\begin{aligned} m^3 &< 377 \times 377 \times 377 < 377 \times 391 \times 589 \\ m^3 &\equiv 1,061,208 \pmod{377 \times 391 \times 589} \end{aligned}$$

Therefore the m^3 calculation cannot have wrap-around. Hence m can be gotten from the ordinary cube root operation. We find

$$(1,061,208)^{1/3} = 102$$

So $m = 102$.

Low Exponent Attack: Example Continued

By e-Theorem

$$1,061,208 \equiv m^3 \pmod{377 \times 391 \times 589}.$$

Most Important Fact Recall that $m < 377$. Hence note that:

$$\begin{aligned} m^3 &< 377 \times 377 \times 377 < 377 \times 391 \times 589 \\ m^3 &\equiv 1,061,208 \pmod{377 \times 391 \times 589} \end{aligned}$$

Therefore the m^3 calculation cannot have wrap-around. Hence m can be gotten from the ordinary cube root operation. We find

$$(1,061,208)^{1/3} = 102$$

So $m = 102$.
Note Cracked RSA without factoring.

Where Did $e = 3$ Come Into This?

Since $m < 377$ we had:

$$m^3 < 377 \times 377 \times 377 < 377 \times 391 \times 589$$

Where Did $e = 3$ Come Into This?

Since $m < 377$ we had:

$$m^3 < 377 \times 377 \times 377 < 377 \times 391 \times 589$$

What if $e = 4$? Then everything goes through until we get to:

$$m^4 < 377 \times 377 \times 377 \times 377$$

We need this to be $< 377 \times 391 \times 589$.

Where Did $e = 3$ Come Into This?

Since $m < 377$ we had:

$$m^3 < 377 \times 377 \times 377 < 377 \times 391 \times 589$$

What if $e = 4$? Then everything goes through until we get to:

$$m^4 < 377 \times 377 \times 377 \times 377$$

We need this to be $< 377 \times 391 \times 589$.
But it's not. So we needed

$$e \leq \text{ The number of people}$$

Low Exponent Attack: Generalized

1) L people. Use $N_1 < \cdots < N_L$. All Rel Prime.
2) $e \leq L$
3) Zelda sends m to L people. Note $m < N_1$.

Low Exponent Attack: Generalized

1) L people. Use $N_1 < \cdots < N_L$. All Rel Prime.
2) $e \leq L$
3) Zelda sends m to L people. Note $m < N_1$.

Can you run the algorithm even if e is not small? **Discuss**

Low Exponent Attack: Generalized

1) L people. Use $N_1 < \cdots < N_L$. All Rel Prime.
2) $e \le L$
3) Zelda sends m to L people. Note $m < N_1$.

Can you run the algorithm even if e is not small? **Discuss**
Yes Run it and if $m^e < N_1 \cdots N_L$ then will still work. You will know it doesn't work if when you need to find an eth root (in $\mathbb{N}$) there is none (in $\mathbb{N}$).

BILL, STOP RECORDING LECTURE!!!!

BILL RECORD LECTURE!!!