BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Low e Attacks on RSA

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
   $0 \leq x < N_1 N_2$:
   $x \equiv a \pmod{N_1}$
   $x \equiv b \pmod{N_2}$
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 $0 \leq x < N_1N_2$:
   $x \equiv a \pmod{N_1}$
   $x \equiv b \pmod{N_2}$
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. $x \equiv y \pmod{N_1N_2}$. (Convention that $0 \leq x < N_1N_2$)

The e Theorem, N_1, N_2 case

Theorem: Assume N_1, N_2 are rel prime, $e, m \in \mathbb{N}$. Let $0 \le x < N_1N_2$ be the number from CRT such that
$x \equiv m^e \pmod{N_1}$
$x \equiv m^e \pmod{N_2}$
Then $x \equiv m^e \pmod{N_1N_2}$. **IF $m^e < N_1N_2$ 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
$x = m^e + k_1 N_1 \qquad k_1 \in \mathbb{Z}$, (Could be negative)
$x = m^e + k_2 N_2 \qquad k_2 \in \mathbb{Z}$, (Could be negative)

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 $k_2 = k N_1$.

The e Theorem, N_1, N_2 case

Theorem: Assume N_1, N_2 are rel prime, $e, m \in \mathbb{N}$. Let $0 \le x < N_1N_2$ be the number from CRT such that
$x \equiv m^e \pmod{N_1}$
$x \equiv m^e \pmod{N_2}$
Then $x \equiv m^e \pmod{N_1N_2}$. **IF** $m^e < N_1N_2$ **then** $x = m^e$**.**

Proof: There exists k_1, k_2 such that
$x = m^e + k_1N_1 \qquad k_1 \in \mathbb{Z}$, (Could be negative)
$x = m^e + k_2N_2 \qquad k_2 \in \mathbb{Z}$, (Could be negative)

$k_1N_1 = k_2N_2$. Since N_1, N_2 rel prime, N_1 divides k_2, so $k_2 = kN_1$.

$x = m^e + kN_1N_2$. Hence $x \equiv m^e \pmod{N_1N_2}$.
If $m^e < N_1N_2$ then since $0 \le x < N_1N_2$ & $x \equiv m^e$, $x = m^e$.

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

The attack can be generalized to $N_1, \ldots, N_L$.
This IS in these slides but we are pressed for time so will skip in lecture.

Advice for Zelda When She Uses RSA

Zelda will use RSA with people $A_1, \ldots, A_L$.
Zelda is sending messages to A_i using $(N_i = p_i q_i, e_i)$

Advice for Zelda When She Uses RSA

Zelda will use RSA with people $A_1, \ldots, A_L$.
Zelda is sending messages to A_i using $(N_i = p_i q_i, e_i)$

1. Make all of the e_i's different

Advice for Zelda When She Uses RSA

Zelda will use RSA with people $A_1, \ldots, A_L$.
Zelda is sending messages to A_i using $(N_i = p_i q_i, e_i)$

1. Make all of the e_i's different
2. Make all of the N_i's different.

Advice for Zelda When She Uses RSA

Zelda will use RSA with people $A_1, \ldots, A_L$.
Zelda is sending messages to A_i using $(N_i = p_i q_i, e_i)$

1. Make all of the e_i's different
2. Make all of the N_i's different.
3. Randomly pad m for NY,NY problem.

Advice for Zelda When She Uses RSA

Zelda will use RSA with people $A_1, \ldots, A_L$.
Zelda is sending messages to A_i using $(N_i = p_i q_i, e_i)$

1. Make all of the e_i's different
2. Make all of the N_i's different.
3. Randomly pad m for NY,NY problem.
4. Randomly pad time to ward off timing attacks.

BILL, STOP RECORDING LECTURE!!!!

BILL STOP RECORDING LECTURE!!!