Public Key Crypto: Low e Attacks on RSA. REDO

Needed Math: Chinese Remainder Theorem Example

Find x such that:

$$\begin{aligned} x &\equiv 17 \pmod{31} \\ x &\equiv 20 \pmod{37} \end{aligned}$$

a) The inverse of 31 mod 37 is 6

b) The inverse of 37 mod 31 is the inverse of 6 mod 31 which is 26.

c) $20 \times 6 \times 31 + 17 \times 26 \times 37 = 20,074$

$$20 \times (31)^{-1} \times 31 + 17 \times (37)^{-1} \times 37$$

Mod 31: First term is 0. Second term is 17. So 17.

Mod 37: First term is 20. Second term is 0. So 20.

So $x = 20,074$ is answer.

Needed Math: Chinese Remainder Theorem Example

Find x such that:

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

So $x = 20{,}074$ is answer. Can we find a smaller x?
We only care about $x \pmod{31}$ and $x \pmod{37}$.
Note:

$$\begin{aligned} x \equiv 17 \pmod{31} &\implies x - 31 \times 37 \equiv 17 \pmod{31} \\ x \equiv 20 \pmod{37} &\implies x - 31 \times 37 \equiv 20 \pmod{37} \end{aligned}$$

If x works then $x - 31 \times 37$ works. Iterate until get between 0 and 31×37. Whats this called? Discuss

Needed Math: Chinese Remainder Theorem Example

Find x such that:

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

So $x = 20,074$ is answer. Can we find a smaller x?
We only care about $x \pmod{31}$ and $x \pmod{37}$.
Note:

$$\begin{aligned} x \equiv 17 \pmod{31} &\implies x - 31 \times 37 \equiv 17 \pmod{31} \\ x \equiv 20 \pmod{37} &\implies x - 31 \times 37 \equiv 20 \pmod{37} \end{aligned}$$

If x works then $x - 31 \times 37$ works. Iterate until get between 0 and 31×37. Whats this called? Discuss $x \pmod{31 \times 37}$

Needed Math: Chinese Remainder Theorem Example

Find x such that:

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

So $x = 20,074$ is answer. Can we find a smaller x?
We only care about $x \pmod{31}$ and $x \pmod{37}$.
Note:

$$\begin{aligned} x &\equiv 17 \pmod{31} &\Longrightarrow\ x - 31 \times 37 &\equiv 17 \pmod{31} \\ x &\equiv 20 \pmod{37} &\Longrightarrow\ x - 31 \times 37 &\equiv 20 \pmod{37} \end{aligned}$$

If x works then $x - 31 \times 37$ works. Iterate until get between 0 and 31×37. Whats this called? Discuss $x \pmod{31 \times 37}$

Upshot: Can take $x = 20,074 \pmod{31 \times 37} = 629$

Needed Math: Chinese Remainder Theorem $L = 2$ Case

1. Input a, b, N_1, N_2, N_1, N_2, rel primes. Want $0 \leq x \leq N_1 N_2$:

$$\begin{aligned} x &\equiv a \pmod{N_1} \\ x &\equiv b \pmod{N_2} \end{aligned}$$

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 $0 \leq x \leq N_1 N_2 - 1$)

Needed Math: The Chinese Remainder Theorem

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

$x \equiv x_1 \pmod{N_1}$

$x \equiv x_2 \pmod{N_2}$

$\vdots$

$x \equiv x_L \pmod{N_L}$

Proof: On HW.

Notation: CRT is Chinese Remainder Theorem.

Needed Math: The e Theorem, $L = 2$ 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

Subtract to get $k_1 N_1 = k_2 N_2$. 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 $0 \le m^e < N_1 N_2$ then since $0 \le x \le N_1 N_2$ & $x \equiv m^e$, $x = m^e$.

Needed Math: The e Theorem, $L = 2$, Example

$N = 31 \times 37 = 1147$. $m = 6$, $e = 4$. Note that $6^4 = 1296 > 1147$.
$x \equiv 6^4 \pmod{31}$
$x \equiv 6^4 \pmod{37}$
$x = 149$. So $149 \equiv 6^4 \pmod{1147}$ but

$$149 = 6^4 - 1147, \text{ so}$$

149 is NOT a power of 4.

Needed Math: The e Theorem, $L = 2$, Example

$N = 31 \times 37 = 1147$. $m = 6$, $e = 4$. Note that $6^4 = 1296 > 1147$.
$x \equiv 6^4 \pmod{31}$
$x \equiv 6^4 \pmod{37}$
$x = 149$. So $149 \equiv 6^4 \pmod{1147}$ but

$$149 = 6^4 - 1147, \text{ so}$$

149 is NOT a power of 4.

$N = 31 \times 37 = 1147$. $m = 5$, $e = 4$. Note that $5^4 = 625 < 1147$.
$x \equiv 5^4 \pmod{31}$
$x \equiv 5^4 \pmod{37}$
$x = 625$. So $625 \equiv 5^4 \pmod{1147}$ but
$625 < 1147$, so $x = 625$ IS a power of 4.

Needed Math: The e Theorem, General L

Theorem: Assume $N_1, \ldots, N_L$ are rel prime, $e, m \in \mathbb{N}$. Assume there is an x (NOT necc $\le N_1 \cdots N_L$) such that

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

Then $x \equiv m^e \pmod{N_1 \cdots N_L}$. If $m^e < N_1 \cdots N_L$ then $x = m^e$.
Proof: Might be on a future HW, or Midterm, or Final, or any combination of the three. Or might not.

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: $x = 1,061,208$.
By e-Theorem

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

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 $m \leq 377$. Hence note that:

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

AH-HA: $m^3 < N_a N_b N_c$. Hence
$x = 1,061,208 = m^3$, so $m = (1,061,208)^{1/3} = 102$
Note: Cracked RSA without factoring.

Where did $e = 3$ Come Into This?

Since $m < 377$ we had:

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

What if $e = 4$ was used? 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 its 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) $e \le L$
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 $m < N_1$.
4) You will finish this on HW. You will write psuedocode.

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 $m < N_1$.
4) You will finish this on HW. You will write psuedocode.

Can you run the algorithm even if e is not small? Discuss
Yes If $m^e < N_1 \cdots N_L$ then it will WORK. But if not then you need to report FAILURE.

Note: If m is small it is possible for $e > L$ but still have $m^e < N_1 \cdots N_L$. Another reason to pad your messages!

Public Key Cryptography: NON-RSA Encryption

RSA

Let n be a security parameter

1. Alice: rand two primes p, q of length n and computes $N = pq$.
2. Alice computes $\phi(N) = \phi(pq) = (p-1)(q-1)$. Denote by R
3. Alice: rand $e \in \{\frac{R}{3}, \ldots, \frac{2R}{3}\}$ that is relatively prime to R. Alice finds d such that $ed \equiv 1 \pmod{R}$.
4. Alice broadcasts (N, e). (Bob and Eve both see it.)
5. Bob: send $m \in \{1, \ldots, N-1\}$, send $m^e \pmod{N}$.
6. Alice gets $m^e \pmod{N}$. She computes

$$(m^e)^d \equiv m^{ed} \equiv m^{ed \pmod{R}} \equiv m^{1 \pmod{R}} \equiv m$$

Is RSA Hard to Crack?

Hardness Assumption (HA) for RSA: The following problem is hard: Given (N, e, c) where $N = pq$ and $c \equiv m^e \pmod{N}$ for some m, Find m.

Objection: HA not natural.
Objection: Contrast:

1. People have been trying to factor QUICKLY since the 1600's. Fermat has the first algorithm I know of.
2. People have been trying to crack RSA since the 1970's.
3. A large part of that effort has been MORE effort on factoring.
4. Caveat: Lots of people, time, money have gone into trying to crack RSA so the contrast is not as clear as it might seem.

Even so:
We Want: An Encryption scheme based on Factoring being hard.

Is there one? Vote: Yes, No, or Unk?

Is RSA Hard to Crack?

Hardness Assumption (HA) for RSA: The following problem is hard: Given (N, e, c) where $N = pq$ and $c \equiv m^e \pmod{N}$ for some m, Find m.

Objection: HA not natural.
Objection: Contrast:

1. People have been trying to factor QUICKLY since the 1600's. Fermat has the first algorithm I know of.
2. People have been trying to crack RSA since the 1970's.
3. A large part of that effort has been MORE effort on factoring.
4. Caveat: Lots of people, time, money have gone into trying to crack RSA so the contrast is not as clear as it might seem.

Even so:
We Want: An Encryption scheme based on Factoring being hard.

Is there one? Vote: Yes, No, or Unk?
Yes. Rabin Encryption.

Rabin Encryption

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod 7$

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod{7}$ $m = 1, 6$

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod 7$ $m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod 7$

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod{7}$ $m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod{7}$ $m = 3, 4$

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod 7$ $m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod 7$ $m = 3, 4$
3. Solve $m^2 \equiv 3 \pmod 7$

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod 7$ $m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod 7$ $m = 3, 4$
3. Solve $m^2 \equiv 3 \pmod 7$ NONE

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod{7}$ $m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod{7}$ $m = 3, 4$
3. Solve $m^2 \equiv 3 \pmod{7}$ NONE
4. Solve $m^2 \equiv 4 \pmod{7}$

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod{7}$ $m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod{7}$ $m = 3, 4$
3. Solve $m^2 \equiv 3 \pmod{7}$ NONE
4. Solve $m^2 \equiv 4 \pmod{7}$ $m = 2, 5$

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod 7$ $m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod 7$ $m = 3, 4$
3. Solve $m^2 \equiv 3 \pmod 7$ NONE
4. Solve $m^2 \equiv 4 \pmod 7$ $m = 2, 5$
5. Solve $m^2 \equiv 5 \pmod 7$

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod{7}$ $m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod{7}$ $m = 3, 4$
3. Solve $m^2 \equiv 3 \pmod{7}$ NONE
4. Solve $m^2 \equiv 4 \pmod{7}$ $m = 2, 5$
5. Solve $m^2 \equiv 5 \pmod{7}$ NONE

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod 7$ $m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod 7$ $m = 3, 4$
3. Solve $m^2 \equiv 3 \pmod 7$ NONE
4. Solve $m^2 \equiv 4 \pmod 7$ $m = 2, 5$
5. Solve $m^2 \equiv 5 \pmod 7$ NONE
6. Solve $m^2 \equiv 6 \pmod 7$

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod{7}$ $m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod{7}$ $m = 3, 4$
3. Solve $m^2 \equiv 3 \pmod{7}$ NONE
4. Solve $m^2 \equiv 4 \pmod{7}$ $m = 2, 5$
5. Solve $m^2 \equiv 5 \pmod{7}$ NONE
6. Solve $m^2 \equiv 6 \pmod{7}$ NONE

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod 7$ $m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod 7$ $m = 3, 4$
3. Solve $m^2 \equiv 3 \pmod 7$ NONE
4. Solve $m^2 \equiv 4 \pmod 7$ $m = 2, 5$
5. Solve $m^2 \equiv 5 \pmod 7$ NONE
6. Solve $m^2 \equiv 6 \pmod 7$ NONE

Math for Rabin Encryption – Square Roots Mod 7

1. Solve $m^2 \equiv 1 \pmod{7}$ $m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod{7}$ $m = 3, 4$
3. Solve $m^2 \equiv 3 \pmod{7}$ NONE
4. Solve $m^2 \equiv 4 \pmod{7}$ $m = 2, 5$
5. Solve $m^2 \equiv 5 \pmod{7}$ NONE
6. Solve $m^2 \equiv 6 \pmod{7}$ NONE

Since $a^2 = (-a)^2$ will *always* have, for all prime p,
$\frac{p-1}{2}$ elements of $\{1, \ldots, p\}$ have sqrts mod p.
$\frac{p-1}{2}$ elements of $\{1, \ldots, p\}$ do not have sqrts mod p.
Note: *Computing Square Roots Mod n* will mean determining if they exists and if so return all of them.

Math for Rabin Encryption – Square Roots Mod p

Theorem: c has a sqrt mod p iff $c^{(p-1)/2} - 1 \equiv 0$.

$$c = m^2 \implies c^{(p-1)/2} \equiv (m^2)^{(p-1)/2} \equiv m^{p-1} \equiv 1.$$

The equation $x^{(p-1)/2} - 1 \equiv 0$ has $(p-1)/2$ roots.
There are $(p-1)/2$ numbers that have sqrts. Hence
If c does not have a sqrt root then $c^{(p-1)/2} - 1 \not\equiv 0$.

Theorem: If $p \equiv 3 \pmod 4$ then easy to compute sqrt mod p.
Given c if $c^{(p-1)/2} \not\equiv 1$ NO. If $\equiv 1$ then:

$$(c^{(p+1)/4})^2 \equiv c^{(p+1)/2} \equiv c(c^{(p-1)/2}) \equiv c \times 1 \equiv c.$$

So output $c^{(p+1)/4}$ and other sqrt is $p - c^{(p+1)/4}$.
Note: If $p \equiv 1 \pmod 4$ also easy to do sqrt.
Upshot: Sqrt mod a prime is easy!

Math for Rabin Encryption – Square Roots Mod n

What about sqrt mod a composite. Try these:

1. Solve $m^2 \equiv 9 \pmod{1147}$
2. Solve $m^2 \equiv 101 \pmod{1147}$

Math for Rabin Encryption – Square Roots Mod n

What about sqrt mod a composite. Try these:

1. Solve $m^2 \equiv 9 \pmod{1147}$
2. Solve $m^2 \equiv 101 \pmod{1147}$

1. Solve $m^2 \equiv 9 \pmod{1147}$:

Math for Rabin Encryption – Square Roots Mod n

What about sqrt mod a composite. Try these:

1. Solve $m^2 \equiv 9 \pmod{1147}$
2. Solve $m^2 \equiv 101 \pmod{1147}$

1. Solve $m^2 \equiv 9 \pmod{1147}$: Answers: 3, 34, 1113, 1144.

Math for Rabin Encryption – Square Roots Mod n

What about sqrt mod a composite. Try these:

1. Solve $m^2 \equiv 9 \pmod{1147}$
2. Solve $m^2 \equiv 101 \pmod{1147}$

1. Solve $m^2 \equiv 9 \pmod{1147}$: Answers: 3, 34, 1113, 1144.
2. Solve $m^2 \equiv 101 \pmod{1147}$:

Math for Rabin Encryption – Square Roots Mod n

What about sqrt mod a composite. Try these:

1. Solve $m^2 \equiv 9 \pmod{1147}$
2. Solve $m^2 \equiv 101 \pmod{1147}$

1. Solve $m^2 \equiv 9 \pmod{1147}$: Answers: 3, 34, 1113, 1144.
2. Solve $m^2 \equiv 101 \pmod{1147}$: Answers: Hmmm.

Math for Rabin Encryption – Square Roots Mod n

What about sqrt mod a composite. Try these:

1. Solve $m^2 \equiv 9 \pmod{1147}$
2. Solve $m^2 \equiv 101 \pmod{1147}$

1. Solve $m^2 \equiv 9 \pmod{1147}$: Answers: 3, 34, 1113, 1144.
2. Solve $m^2 \equiv 101 \pmod{1147}$: Answers: Hmmm.

Solve $m^2 \equiv 9 \pmod{1147}$: 3, $1147 - 3 = 1144$ easy. If had 34 then $1147 - 34 = 1144$ easy. But how to get 34?

Vote: Is finding sqrts mod N hard? Yes, No, Unk?

Math for Rabin Encryption – Square Roots Mod n

What about sqrt mod a composite. Try these:

1. Solve $m^2 \equiv 9 \pmod{1147}$
2. Solve $m^2 \equiv 101 \pmod{1147}$

1. Solve $m^2 \equiv 9 \pmod{1147}$: Answers: 3, 34, 1113, 1144.
2. Solve $m^2 \equiv 101 \pmod{1147}$: Answers: Hmmm.

Solve $m^2 \equiv 9 \pmod{1147}$: 3, $1147 - 3 = 1144$ easy. If had 34 then $1147 - 34 = 1144$ easy. But how to get 34?

Vote: Is finding sqrts mod N hard? Yes, No, Unk?
Unk: Many computational questions in Number Theory are Unk.

$m^2 \equiv 101 \pmod{1147}$ $1147 = 31 * 37$

$m^2 \equiv 101 \pmod{31}$. $m^2 \equiv 8 \pmod{31}$: $m \equiv \pm 15 \pmod{31}$
$m^2 \equiv 101 \pmod{37}$. $m^2 \equiv 27 \pmod{37}$ $m \equiv \pm 8 \pmod{37}$.
One approach: Want number $m \in \{1, \ldots, 1146\}$ such that
$m \equiv 15 \pmod{31}$
$m \equiv 8 \pmod{37}$
Use CRT to get:

$$m = 15918 \equiv 1007 \pmod{1147}$$

Math for Rabin Encryption – Square Roots Mod n

By using $\pm 15 \pmod{31}$ and $\pm 8 \pmod{37}$ can find 4 sqrts.

Upshot: sqrts mod N easy if know the factors of n.
Upshot: Always get 0 or 2 or 4 sqrts if mod $N = pq$.

What about finding sqrts mod N where factors of N are not known?

Math for Rabin Encryption – Square Roots Mod n

By using $\pm 15 \pmod{31}$ and $\pm 8 \pmod{37}$ can find 4 sqrts.

Upshot: sqrts mod N easy if know the factors of n.
Upshot: Always get 0 or 2 or 4 sqrts if mod $N = pq$.

What about finding sqrts mod N where factors of N are not known?
Normally I would say
The problem of finding sqrt mod N where the factors of N are not known is believed to be hard.

Math for Rabin Encryption – Square Roots Mod n

By using $\pm 15 \pmod{31}$ and $\pm 8 \pmod{37}$ can find 4 sqrts.

Upshot: sqrts mod N easy if know the factors of n.
Upshot: Always get 0 or 2 or 4 sqrts if mod $N = pq$.

What about finding sqrts mod N where factors of N are not known?
Normally I would say
The problem of finding sqrt mod N where the factors of N are not known is believed to be hard.
This time I can say something stronger.

Math for Rabin Encryption – Square Roots Mod n

How hard is sqrts mod N when factors of N not known?

Math for Rabin Encryption – Square Roots Mod n

How hard is sqrts mod N when factors of N not known?

Theorem: If finding sqrts mod N is easy then factoring is easy.

1. Given $N = pq$ (p, q unknown) want to factor it.
2. Pick a rand c and find its sqrts.
3. If it doesn't have ≥ 4 sqrts then goto step 2.
4. The four sqrts are of the form $\pm x$ and $\pm y$. Now use x, y. We know that

$$x^2 \equiv y^2 \pmod{N}.$$

$$x^2 - y^2 \equiv 0 \pmod{N}$$

$$(x - y)(x + y) \equiv 0 \pmod{N}$$

$GCD(x - y, N)$ or $GCD(x + y, N)$ likely factor.

Discuss: Why did I use x, y instead of $x, -x$?

All you Need to Know for Rabin's Scheme

1. Finding primes is easy.
2. Squaring is easy.
3. If N is factored then sqrt mod N is easy.
4. If N is not factored then sqrt mod N is thought to be hard (equiv fo factoring).

Rabin's Encryption Scheme

n is a security parameter

1. Alice gen p, q primes of length n. Let $N = pq$. Send N.
2. Encode: To send m, Bob sends $c = m^2 \pmod{N}$.
3. Decode: Alice can find m such that $m^2 \equiv c \pmod{N}$.

Rabin's Encryption Scheme

n is a security parameter

1. Alice gen p, q primes of length n. Let $N = pq$. Send N.
2. Encode: To send m, Bob sends $c = m^2 \pmod{N}$.
3. Decode: Alice can find m such that $m^2 \equiv c \pmod{N}$. OH! There will be two or four of them! What to do? Later.

Rabin's Encryption Scheme

n is a security parameter

1. Alice gen p, q primes of length n. Let $N = pq$. Send N.
2. Encode: To send m, Bob sends $c = m^2 \pmod{N}$.
3. Decode: Alice can find m such that $m^2 \equiv c \pmod{N}$. OH! There will be two or four of them! What to do? Later.

PRO: Easy for Alice and Bob
BIG PRO: Factoring Hard is hardness assumption.
CON: Alice has to figure out which of the sqrts is correct message.
Caveat: If m is English text then Alice can tell which one it is.
Caveat: If not. Hmmm.

How to Modify Rabin's Encryption?

Lets looks at mod $21 = 3 * 7$.

$1^2, 8^2, 13^2, 20^2 \equiv 1$

$2^2, 5^2, 16^2, 19^2 \equiv 4$

$3^2, 18^2 \equiv 9$

$4^2, 10^2, 11^2, 17^2 \equiv 16$

$6^2, 15^2 \equiv 15$

$7^2, 14^2 \equiv 7$

$9^2, 12^2 \equiv 18$

Question: What do the red numbers have in common? Discuss

How to Modify Rabin's Encryption?

Lets looks at mod $21 = 3 * 7$.

$1^2, 8^2, 13^2, 20^2 \equiv 1$

$2^2, 5^2, 16^2, 19^2 \equiv 4$

$3^2, 18^2 \equiv 9$

$4^2, 10^2, 11^2, 17^2 \equiv 16$

$6^2, 15^2 \equiv 15$

$7^2, 14^2 \equiv 7$

$9^2, 12^2 \equiv 18$

Question: What do the red numbers have in common? Discuss

They all have square roots! They are all also on the RHS.

How to Modify Rabin's Encryption?

Lets looks at mod $21 = 3 * 7$.

$1^2, 8^2, 13^2, 20^2 \equiv 1$

$2^2, 5^2, 16^2, 19^2 \equiv 4$

$3^2, 18^2 \equiv 9$

$4^2, 10^2, 11^2, 17^2 \equiv 16$

$6^2, 15^2 \equiv 15$

$7^2, 14^2 \equiv 7$

$9^2, 12^2 \equiv 18$

Question: What do the red numbers have in common? Discuss

They all have square roots! They are all also on the RHS.

What is it about 21 that makes this work?

A Theorem from Number Theory

Definition: A *Blum Int* is product of two primes $\equiv 3 \pmod 4$.
Example: $21 = 3 \times 7$.

Notation: SQ_N is the set of squares mod N. (Often called QR_N.)
Example: If $N = 21$ then $SQ_N = \{1, 4, 7, 9, 15, 16, 18\}$.

Theorem: Assume N is a Blum Integer. Let $m \in SQ_N$. Then of the two or four sqrts of m, only one is itself in SQ_N.
Proof: Omitted. Note: (1) not that hard, and (2) in Katz book.

We use Theorem to modify Rabin Encryption.

Rabin's Encryption Scheme 2.0

(This modification by Blum and Williams BW.) n is sec param.

1. Alice gen p, q primes of length n such that $p, q \equiv 3 \pmod 4$. Let $N = pq$. Send N.
2. Encode: To send $m \in SQ_N$, Bob sends $c = m^2 \pmod N$.
3. Decode: Alice can find 2 or 4 m such that $m^2 \equiv c \pmod N$. Take the $m \in SQ_N$.

PRO: Easy for Alice and Bob
Biggest PRO: Factoring Hard is Hardness Assumption (HA)
CON: Messages have to be in SQ_N.

HA for Rabin's Encryption Scheme 1.0, 2.0

HA1 for Rabin 1.0: Given $N = pq$, $m^2 \pmod{N}$, finding m is hard.

Good News: HA1 equiv to: Given $N = pq$, factoring it is hard.

HA2 for Rabin 2.0: Given $N = pq$, $p, q \equiv 3 \pmod{4}$, $m^2 \pmod{N}$, $m \in SQ_N$, finding m is hard.

Good News: HA2 equiv to: Given $N = pq$, $p, q \equiv 3 \pmod{4}$, factoring it is hard.

Caveat: The above only applies to ciphertext-only attacks. Eve sees what Bob sends. What if Eve could do more?

Can Rabin's Encryption Scheme Can Be Cracked?

n is a security parameter

1. Alice gen p, q primes of length n. Let $N = pq$. Send N.
2. Encode: To send m, Bob sends $c = m^2 \pmod{N}$.
3. Decode: Alice can find m such that $m^2 \equiv c \pmod{N}$. Picks a poss out somehow.

Vote: Crackable, Uncrackable, Unk

Can Rabin's Encryption Scheme Can Be Cracked?

n is a security parameter

1. Alice gen p, q primes of length n. Let $N = pq$. Send N.
2. Encode: To send m, Bob sends $c = m^2 \pmod{N}$.
3. Decode: Alice can find m such that $m^2 \equiv c \pmod{N}$. Picks a poss out somehow.

Vote: Crackable, Uncrackable, Unk

Crackable:

Attack!: Eve picks an m and tricks Alice into sending message m via $m^2 \equiv c$. Eve is hoping that Bob will find *another* sqrt of m^2. Say Alice gets m'. Then

$m^2 - (m')^2 \equiv 0 \pmod{N}$.

$(m - m')(m + m') \equiv 0 \pmod{N}$.

$m - m'$ or $m + m'$ may share factors with N so do $gcd(m - m', N)$ and $gcd(m + m', N)$. Can factor N and hence – game over!

What else to known

1. Original scheme had problem of which sqrt. BW fixed this but by then RSA was pervasive.
2. RSA & Rabin both have issues that require padding.
3. RSA & Rabin both have attacks.
4. There are variants of Rabin that thwarts the attack above. (a) one of them only allows 1 bit at a time, (b) one of them is not provably equiv to factoring.
5. RSA solved its problems. Rabin could have (or perhaps did).

Alternate History: Had timing been different Rabin would have been the one everyone uses.

Goldwasser-Micali (GM) Encryption

Math Needed For GM Encryption

Definition

1. SQ_N is a number in $\mathbb{Z}_N$ that does have a sqrt mod N
2. NSQ_N is a number in $\mathbb{Z}_N$ that does not have a sqrt mod N (often called QNR_N).

Discuss: Let $N = 35$. Find all elements of SQ_N and NSQ_N.

Math Needed For GM Encryption

1. Given n, can gen rand primes of length n easily.
2. Given p, q let $N = pq$. Can gen a rand $z \in NSQ_N$ easily.
3. $SQ_N \times SQ_N = SQ_N$.
4. $NSQ_N \times SQ_N = NSQ_N$.
5. Given p, q, c can determine if c is in SQ_{pq} easily.
6. Given N, c determining if $c \in SQ_N$ seems hard.

Discuss: Lets do some examples mod 35! (thats not a factorial, I'm excited about doing examples!)

GM Encryption

n is a security parameter. Will only send ONE bit. Bummer!

1. Alice: rand p, q primes of length n, $z \in NSQ_N$. Computes $N = pq$. Send (N, z).
2. Encode: To send $m \in \{0, 1\}$, Bob: rand $x \in \mathbb{Z}_N$, sends $c = z^m x^2 \pmod{N}$. Note that:
   2.1 If $m = 0$ then $z^m x^2 = x^2 \in SQ_N$.
   2.2 If $m = 1$ then $z^m x^2 = zx^2 \in NSQ_N$.
3. Decode: Alice determines if $c \in SQ$ or not. If YES then $m = 0$. If NO then $m = 1$.

BIG PRO: Hardness assumption natural – next slide.

BIG CON: Messages have to be 1-bit long.

TIME: For one bit you need $4 \log N$ steps.

GM Encryption Hardness Assumption (HA)

SQ problem: Given (c, N) determine if $c \in SQ_N$.
HA: The SQ problem is computationally hard.
Note: SQ problem has been studied by Number Theorists for a long time way before there was crypto. Hence it is a natural problem.

PRO: SQ is legit, well studied (unlike RSA assumption)
CON: SQ studied by Number Theorists, not computationally.

Back to GM:
BIGGEST CON: They take life one bit at a time. Really?

Blum-Goldwasser Encryption

Math You Need For Blum-Goldwasser Encryption

Definition

1. SQ_N is a number in $\mathbb{Z}_N$ that does have a sqrt mod N
2. NSQ_N is a number in $\mathbb{Z}_N$ that does not have a sqrt mod N

Math You Need For Blum-Goldwasser Encryption

(You have seen this before but good review.)

1. Given n, can gen rand primes of length n easily.
2. Given p, q let $N = pq$. Can gen a rand $z \in NSQ_N$ easily.
3. $SQ_N \times SQ_N = SQ_N$.
4. $NSQ_N \times SQ_N = NSQ_N$.
5. Given p, q, c can determine if c is in SQ_{pq} easily.
6. Given N, c determining if $c \in SQ_N$ seems hard.
7. $LSB(x)$ is the least sig bit of x.

Blum-Goldwasser Enc. n Sec Param, L length of msg

1. Alice: p, q primes len n, $p, q \equiv 3 \pmod 4$. $N = pq$. Send N.
2. Encode: Bob sends $m \in \{0,1\}^L$: rand $r \in \mathbb{Z}_N$

$$
\begin{array}{rll}
x_1 = r^2 & \bmod N & b_1 = LSB(x_1) \\
x_2 = x_1^2 & \bmod N & b_2 = LSB(x_2) \\
\vdots & \vdots & \vdots \quad \vdots \quad \vdots \\
x_L = x_{L-1}^2 & \bmod N & b_L = LSB(x_L)
\end{array}
$$

   Send $c = ((m_1 \oplus b_1, \ldots, m_L \oplus b_L), x_L)$.
3. Decode: From x_L Alice gets x_{L-1}, …, x_1 by sqrt (since Alice has p, q), then $b_1, \ldots, b_L$, then $m_1, \ldots, m_L$.

BIG PRO: Hardness assumption – next slide.
TIME: For L bits need $(L+3)\log N$ steps. Better than GM.

Blum-Goldwasser Encryption Hardness Assumption (HA)

The sequence $b_0, b_1, \ldots, b_L$ is the output of a known psuedorandom generator called BBS (Blum-Blum-Shub).

BBS problem: Given x_L compute $b_L, \ldots, b_1$.

HA: *BBS* is computationally hard.

PRO: Natural in that *BBS* predates the cipher.
CON: *BBS* has not been around that long.