Low $e$ Attacks on RSA
1. Zelda is sending messages to Alice using $N_a = 377$, $e = 3$.
2. Zelda is sending messages to Bob using $N_b = 391$, $e = 3$.
3. Zelda is sending messages to Carol using $N_c = 589$, $e = 3$.

$e$ 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 $N_b = 391$, $e = 3$.
3. Zelda is sending messages to Carol using $N_c = 589$, $e = 3$.

$e$ is low. That will make the system crackable if ... Zelda sends same $m$ to all three. Note $m < 377$. 
1. Zelda is sending messages to Alice using $N_a = 377$, $e = 3$.
2. Zelda is sending messages to Bob using $N_b = 391$, $e = 3$.
3. Zelda is sending messages to Carol using $N_c = 589$, $e = 3$.

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

Zelda sends *same* $m$ to all three. **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.
Scenario

1. Zelda is sending messages to Alice using $N_a = 377$, $e = 3$.
2. Zelda is sending messages to Bob using $N_b = 391$, $e = 3$.
3. Zelda is sending messages to Carol using $N_c = 589$, $e = 3$.

$e$ is low. That will make the system crackable if … Zelda sends *same $m$* to all three. **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.

We will develop the math and the attack. Called a low-$e$ attack.
Needed Math: 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.
c)

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

$x \pmod{31}$: First term is 0. Second term is 17. So 17.
$x \pmod{37}$: 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:

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

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

Note:

$$x \equiv 17 \pmod{31} \implies x - 31 \times 37 \equiv 17 \pmod{31}$$
$$x \equiv 20 \pmod{37} \implies x - 31 \times 37 \equiv 20 \pmod{37}$$

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

$$20,074 \pmod{31 \times 37} = 629.$$ 

Upshot: Can take $x = 20,074 \pmod{31 \times 37} = 629$
What if \( x = m^2 \) is a Square?

Find \( m \) such that:

\[
m^2 \equiv 8 \pmod{17} \quad \& \quad m^2 \equiv 25 \pmod{37}
\]

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:

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

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:

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

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

$$m^2 = 12 \times 37 \times 6 + 16 \times 17 \times 24 = 9192$$

9192 $\equiv 386 \pmod{17 \times 37}$.
What if \( x = m^3 \)?

Find \( m \) such that:

\[
\begin{align*}
m^3 &\equiv 12 \pmod{17} \quad &\& \quad m^3 &\equiv 16 \pmod{37}
\end{align*}
\]

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

\[
m^2 = 12 \times 37 \times 6 + 16 \times 17 \times 24 = 9192
\]

\[
9192 \equiv 386 \pmod{17 \times 37}.
\]

OH, \( m^3 \equiv 386 \). This is NOT a cube. So the method does not always work.

What was different?
Squares and Cubes

Find \( m \) such that:

\[
m^2 \equiv 8 \pmod{17} \quad \& \quad m^2 \equiv 25 \pmod{37}
\]

The message \( m \) is \( \leq 17 \) and \( \leq 37 \). So \( m^2 \leq 17 \times 37 \). So \( m^2 \equiv m^2 \pmod{17 \times 37} \) (no reduce).
Find $m$ such that:

\[ m^2 \equiv 8 \pmod{17} \quad \& \quad m^2 \equiv 25 \pmod{37} \]

The message $m$ is $\leq 17$ and $\leq 37$. So
\[ m^2 \leq 17 \times 37. \] So $m^2 \equiv m^2 \pmod{17 \times 37}$ (no reduce).

Find $m$ such that:

\[ m^3 \equiv 12 \pmod{17} \quad \& \quad m^3 \equiv 16 \pmod{37} \]

The message $m$ is $\leq 17$ and $\leq 37$. But
\[ m^3 \geq 17 \times 37. \] So $m^3 \pmod{17 \times 37}$ DOES reduce.
Squares and Cubes

Find \( m \) such that:

\[
m^2 \equiv 8 \pmod{17} \quad \& \quad m^2 \equiv 25 \pmod{37}
\]

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

Find \( m \) such that:

\[
m^3 \equiv 12 \pmod{17} \quad \& \quad m^3 \equiv 16 \pmod{37}
\]

The message \( m \) is \( \leq 17 \) and \( \leq 37 \). But \( m^3 \geq 17 \times 37 \). So \( m^3 \pmod{17 \times 37} \) DOES reduce. We return to this point in a few slides.
Needed Math: Chinese Remainder Theorem \( L = 2 \) Case

1. Input \( a, b, N_1, N_2, N_1, N_2 \), rel primes. Want \( 0 \leq x \leq N_1 N_2 \):
   \[
   x \equiv a \pmod{N_1} \\
   x \equiv b \pmod{N_2}
   \]

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 \( 0 \leq x \leq N_1 N_2 - 1 \))
Theorem: If $N_1, \ldots, N_L$ are rel prime, $x_1, \ldots, x_L$ are anything, then there exists $x$ with $0 \leq x \leq N_1 \cdots N_L$ 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: Omitted.

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 $0 \leq x < N_1 N_2$ 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

$x = m^e + k_1 N_1$ \hspace{1cm} $k_1 \in \mathbb{Z}$, Could be negative

$x = m^e + k_2 N_2$ \hspace{1cm} $k_2 \in \mathbb{Z}$, 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 $0 \leq m^e < N_1 N_2$ then since $0 \leq x \leq N_1 N_2$ & $x \equiv m^e$, $x = m^e$. 
Theorem: Assume $N_1, \ldots, N_L$ are rel prime, $e, m \in \mathbb{N}$. 

$$x \equiv m^e \pmod{N_1}$$

$$\vdots$$

$$x \equiv m^e \pmod{N_L}$$

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

Proof: Use CRT to find $x$ such that

$$x \equiv m^e \pmod{N_1}$$
$$\vdots$$
$$x \equiv m^e \pmod{N_L}$$

and $0 \leq x \leq N_1 \cdots N_L$. 

Since $m \leq N_i$ and $e \leq L$, $m^e \leq N_1 \cdots N_L$.

Hence $x$ is an eth power in $\mathbb{N}$. Take the eth root to find $m$.

End of Proof
Low Exponent Attack: Example

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 \( 0 \leq x < 377 \times 391 \times 589 \).
\[
x \equiv 330 \equiv m^3 \pmod{377}
\]
\[
x \equiv 34 \equiv m^3 \pmod{391}
\]
\[
x \equiv 419 \equiv m^3 \pmod{589}
\]
Eve finds such a number: \( x = 1,061,208 \).
By \( e \)-Theorem

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

\[
\begin{align*}
m^3 &< 377 \times 377 \times 377 < 377 \times 391 \times 589 \\
m^3 &\equiv 1,061,208 \pmod{377 \times 391 \times 589}
\end{align*}
\]

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:

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

What is $e = 4$ 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 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 $m < N_1$. 

4) You will finish this on HW. You will write psuedocode.

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

Yes – and if $m$ is small enough it may even work. But it needs to report FAILURE if get $x > N_1 \cdots N_L$. 
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) $e \leq L$
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
Yes- and if $m$ is small enough it may even work. But it needs to
report FAILURE if get $x > N_1 \cdots N_L$. 
Public Key Cryptography: NON-RSA Encryption
RSA

Let $n$ be a security parameter

1. Alice picks 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 picks an $e \in \{\frac{R}{3}, \ldots, \frac{2R}{3}\}$ 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: To send $m \in \{1, \ldots, N-1\}$, send $m^e \pmod{N}$.
6. If Alice gets $m^e \pmod{N}$ she computes

\[(m^e)^d \equiv m^{ed} \equiv m^{ed} \pmod{R} \equiv m^1 \pmod{R} \equiv m\]
Yet Another RSA attack
Review of RSA Attacks

1. If $N$ is small, Eve Factors. **Response:** Use $p, q$ large.
2. If same $e$, $e \leq L$. Low-$e$ attack. **Response:** Large $e$.
3. If same $e$, $m^e < N_1 \cdots N_L$. Low-$e$ attack. **Response:** Pad $m$.
4. NY,NY problem. Leaks info. **Response:** Rand Pad $m$.
5. Timing Attacks: **Response:** Rand Pad time.

Note items 2 and 3:

- $e$ same but $N$’s Different

How about

- $N$ same but $e$’s Different

Surely that can’t be a problem!
Review of RSA Attacks

1. If $N$ is small, Eve Factors. **Response:** Use $p, q$ large.
2. If same $e$, $e \leq L$. Low-$e$ attack. **Response:** Large $e$.
3. If same $e$, $m^e < N_1 \cdots N_L$. Low-$e$ attack. **Response:** Pad $m$.
4. NY,NY problem. Leaks info. **Response:** Rand Pad $m$.
5. Timing Attacks: **Response:** Rand Pad time.

Note items 2 and 3:

- $e$ same but $N$’s Different

How about

- $N$ same but $e$’s Different

Surely that can’t be a problem!

Or can it!
Review of RSA Attacks

1. If $N$ is small, Eve Factors. **Response:** Use $p, q$ large.
2. If same $e$, $e \leq L$. Low-$e$ attack. **Response:** Large $e$.
3. If same $e$, $m^e < N_1 \cdot \cdot N_L$. Low-$e$ attack. **Response:** Pad $m$.
4. NY,NY problem. Leaks info. **Response:** Rand Pad $m$.
5. Timing Attacks: **Response:** Rand Pad time.

Note items 2 and 3:

- $e$ same but $N$’s Different

How about

- $N$ same but $e$’s Different

Surely that can’t be a problem!
Or can it!
Won’t bother with a vote, onto the next slide.
Same $N$, Different $e$, Eve Cracks RSA

1. Alice gives $B_1 (N, e_1)$
2. Alice gives $B_2 (N, e_2)$
3. $e_1, e_2$ are rel prime (Bad idea?).

Alice sends $m$ to both $B_1$ and $B_2$. Eve sees

1. $m^{e_1} \pmod{N}$
2. $m^{e_2} \pmod{N}$
Same $N$, Different $e$, Eve Cracks RSA

1. Alice gives $B_1 (N, e_1)$
2. Alice gives $B_2 (N, e_2)$
3. $e_1, e_2$ are rel prime (Bad idea?).

Alice sends $m$ to both $B_1$ and $B_2$. Eve sees

1. $m^{e_1} \pmod{N}$
2. $m^{e_2} \pmod{N}$

$e_1, e_2$ rel prime, so $\exists x, y \in \mathbb{Z} \ e_1x + e_2y = 1$. 

Caveat: if (say) $x < 0$ need $m^{e_1}$ to have inverse mod $N$.

Note: Eve found $m$ without factoring $N$.

Response: Use Different $N$. 
Same $N$, Different $e$, Eve Cracks RSA

1. Alice gives $B_1 (N, e_1)$
2. Alice gives $B_2 (N, e_2)$
3. $e_1, e_2$ are rel prime (Bad idea?).

Alice sends $m$ to both $B_1$ and $B_2$. Eve sees

1. $m^{e_1} \pmod{N}$
2. $m^{e_2} \pmod{N}$

$e_1, e_2$ rel prime, so $\exists x, y \in \mathbb{Z} \ e_1 x + e_2 y = 1$. Eve finds $x, y$ with Euclidean Algorithm and then:

$$(m^{e_1})^x \times (m^{e_2})^y \pmod{N} = m^{e_1 x + e_2 y} \pmod{N} = m \pmod{N}$$

Caveat: if (say) $x < 0$ need $m^{e_1}$ to have inverse mod $N$.

Note: Eve found $m$ without factoring $N$.

Response: Use Different $N$. 

Advice for Alice When she uses RSA

Alice will use RSA with people $A_1, \ldots, A_L$. Will use $(N_i = p_i q_i, e_i)$ for $A_i$.

1. Pick $p_i, q_i$ large and different.
2. Can have all $e_i$’s the same $e$ but should be large.
3. Randomly Pad $m$
4. Randomly pad time
Is RSA Hard to Crack?

Hardness Assumption 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: Hardness assumption not natural.
Objection: Hardness assumption does not have a long history of being tested.
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 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: Hardness assumption not natural.
Objection: Hardness assumption does not have a long history of being tested.
We Want: An Encryption scheme based on Factoring being hard.

Is there one? **Vote:** Yes, No, or Unk?
Yes. Rabin Encryption.
Rabin Encryption
1. Solve $m^2 \equiv 1 \pmod{7}$
1. Solve $m^2 \equiv 1 \pmod{7}$ $m = 1, 6$

Since $a^2 = (-a)^2$ will always have, for all prime $p$, $p-1$ elements of \{1, ..., $p$\} have sqrts mod $p$. $p-1$ elements of \{1, ..., $p$\} do not have sqrts mod $p$.

Note: Computing Square Roots Mod $n$ will mean determining if they exist and if so return all of them.
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 \( m^2 \equiv 2 \pmod{7} \) \( m = 3, 4 \)
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 \( m^2 \equiv 1 \) (mod 7) \( m = 1, 6 \)
2. Solve \( m^2 \equiv 2 \) (mod 7) \( m = 3, 4 \)
3. Solve \( m^2 \equiv 3 \) (mod 7) NONE
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 $m^2 \equiv 4 \pmod{7}$

Since $a^2 = (-a)^2$ will always have, for all prime $p$, $p-1$ elements of $\{1, \ldots, p\}$ have sqrts mod $p$.

$p-1$ elements of $\{1, \ldots, p\}$ do not have sqrts mod $p$.

Note: Computing Square Roots Mod $n$ will mean determining if they exist and if so return all of them.
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 \( m^2 \equiv 5 \pmod{7} \)
1. Solve $m^2 \equiv 1 \pmod{7} \Rightarrow m = 1, 6$
2. Solve $m^2 \equiv 2 \pmod{7} \Rightarrow m = 3, 4$
3. Solve $m^2 \equiv 3 \pmod{7} \Rightarrow \text{NONE}$
4. Solve $m^2 \equiv 4 \pmod{7} \Rightarrow m = 2, 5$
5. Solve $m^2 \equiv 5 \pmod{7} \Rightarrow \text{NONE}$
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 \( m^2 \equiv 6 \pmod{7} \)
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 $p$, $p^2 - 1$ elements of \{1, ..., p\} have sqrts mod $p$. $p^2 - 1$ elements of \{1, ..., 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 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 $p$,
$p-1 \over 2$ elements of $\{1, \ldots, p\}$ have sqrts mod $p$.
$p-1 \over 2$ 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 $p \equiv 1 \pmod{4}$ easy to do sqrt. We omit.

**Upshot:** Sqrt mod a prime is easy!
Math for Rabin Encryption – Procedures

How to find square roots mod $p$ if $p \equiv 3 \pmod{4}$:
All arithmetic is mod $p$.

Input($c$)
Compute $c^{(p-1)/2}$. If it is NOT 1 then output There is no square root!. If it is 1 then goto next step
Compute $a = c^{(p+1)/4}$.
Output $a$ and $p - a$. These are the two square roots.

Note: There is a similar algorithm for $p \equiv 1 \pmod{4}$ but it is slightly more complicated.
What about sqrt mod a composite. Try these:

1. Solve $m^2 \equiv 9 \pmod{1147}$
   - Answers: 3, 1147 - 3 = 1144 easy. If had 34 then 1147 - 34 = 1144 easy. But how to get 34?
2. Solve $m^2 \equiv 101 \pmod{1147}$:
   - Hmmm.

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

Unk: Many computational questions in Number Theory are Unk.
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, 1147
2. Solve $m^2 \equiv 101 \pmod{1147}$: 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.
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.

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

Unk: Many computational questions in Number Theory are Unk.
What about sqrt mod a composite. Try these:

1. Solve \( m^2 \equiv 9 \) (mod 1147)
2. Solve \( m^2 \equiv 101 \) (mod 1147)

1. Solve \( m^2 \equiv 9 \) (mod 1147): Answers: 3, 34, 1113, 1144.
2. Solve \( m^2 \equiv 101 \) (mod 1147):
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: Hmm.
What about sqrt mod a composite. Try these:

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?
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.
\[ m^2 \equiv 101 \pmod{1147} \]
\[ 1147 = 31 \times 37 \]

\[ m^2 \equiv 101 \pmod{31} \]
\[ m^2 \equiv 8 \pmod{31} \]
\[ m \equiv \pm 15 \pmod{31} \]

\[ m^2 \equiv 101 \pmod{37} \]
\[ m^2 \equiv 27 \pmod{37} \]
\[ m \equiv \pm 8 \pmod{37} \]

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:

\[ m = 15918 \equiv 1007 \pmod{1147} \]
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?
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.
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?

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 random \( c \) and find its sqrts.
3. If it doesn't have \( \geq 4 \) 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 \( x^2 \equiv y^2 \pmod{N} \).

\[ x^2 - y^2 \equiv 0 \pmod{N} \]
\[ (x-y)(x+y) \equiv 0 \pmod{N} \]

\( \text{GCD}(x-y, N) \) or \( \text{GCD}(x+y, N) \) likely factor.

Discuss: Why did I use \( x, y \) instead of \( x, -x \)?
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 random \( c \) and find its sqrts.
3. If it doesn’t have \( \geq 4 \) 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 to 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 $m^2 \equiv c \pmod{N}$. 

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.
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.
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. Hmm.
How to Modify Rabin’s Encryption?

Let's look at mod $21 = 3 \times 7$.

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

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

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

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

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

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

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

**Question:** What do the red numbers have in common? **Discuss**
How to Modify Rabin’s Encryption?

Lets looks at mod $21 = 3 \times 7$.

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

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

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

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

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

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

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

**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?

Let's look at mod $21 = 3 \times 7$.

$1^2, 8^2, 13^2, 20^2 \equiv 1$
$2^2, 5^2, 16^2, 19^2 \equiv 4$
$3^2, 18^2 \equiv 9$
$4^2, 10^2, 11^2, 17^2 \equiv 16$
$6^2, 15^2 \equiv 15$
$7^2, 14^2 \equiv 7$
$9^2, 12^2 \equiv 18$

**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 srqts of \( m \), only one is itself in \( SQ_N \).
Proof: Omitted

We use Theorem to modify Rabin Encryption.
Rabin’s Enc Scheme 2.0—by Blum and Williams.

\( n \) is a security parameter.

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 \( m \), Bob sends \( c = m^2 \pmod{N} \). Only send \( m \)'s in \( SQ_N \).

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.

**CON:** Messages have to be in \( SQ_N \).
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!
Another way To Make Rabin Unique

Recall Rabin’s 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 \( m^2 \equiv c \pmod{N} \).
Another way To Make Rabin Unique

Recall Rabin’s 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?
Making Rabin Unique. We call it RabinU

1. Alice gen $p,q$ primes of length $n$. Let $N = pq$. NEW: Let $x$ be a random element of $NSQ_N$. Send $(N,x)$.

2. Encode: To send $m$, Bob sends
   2.1 $c = m + xm^{-1} \pmod{N}$,
   2.2 0 if $m \in SQ_N$, 1 if $m \in NSQ_N$, and
   2.3 0 if $(cm^{-1} \pmod{N} > m)$, 1 if $(cm^{-1} \pmod{N} < m)$.

3. Decode: Alice needs $m$ st $c = m + xm^{-1}$, so solve $m^2 - cm + c = 0$. This gives 2 or 4 roots. The info about $m \in SQ_N$ and $cm^{-1} \pmod{N} < m$ uniquely determines which root. (We skip details)

Note: RabinU can be cracked iff Factoring is easy.
What else to known

1. Alice may need to guess which of the 2 or 4 possible messages is the one to use, which is why it's not used. Blum and Williams showed how to make the message unique, but by the time they did RSA was pervasive.

2. RSA and Rabin have similar issues which require padding-randomness

3. RSA has also had attacks as we've seen.

4. Rabin can be cracked with Chosen Plaintext Attack.

5. There is a variant of Rabin that thwarts the CPA but not provably equiv to factoring.

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