I just finished season one of *Killing Eve*. Eve works for MI-5 and is tracking a female assassin who is also a psychopath. Two interesting points, one relevant to this course, one not.
I just finished season one of *Killing Eve*. Eve works for MI-5 and is tracking a female assassin who is also a psychopath. Two interesting points, one relevant to this course, one not.

Eve’s pin numbers is 1-2-3-4
I just finished season one of *Killing Eve*. Eve works for MI-5 and is tracking a female assassin who is also a psychopath. Two interesting points, one relevant to this course, one not.

Eve’s pin numbers is 1-2-3-4

**Eve to Psychopath** You’re a psychopath.
I just finished season one of *Killing Eve*. Eve works for MI-5 and is tracking a female assassin who is also a psychopath. Two interesting points, one relevant to this course, one not.

Eve’s pin numbers is 1-2-3-4

**Eve to Psychopath** You’re a psychopath.  
**Psychopath to Eve** You should never call a psychopath a psychopath. It’s gets them angry.
Other Public Key Encryption Schemes

October 14, 2019
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 has withstood attempts to show its false since 1976. Note that much time
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 has withstood attempts to show its false since 1976. Note that much time
We Want: An Encryption scheme based on Factoring being hard. Factoring (1) is a more natural problem and (2) has been studied for far longer.

Is there one? Vote: Yes, No, or Unknown?
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 has withstood attempts to show its false since 1976. Note that much time
We Want: An Encryption scheme based on Factoring being hard.
Factoring (1) is a more natural problem and (2) has been studied for far longer.

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

October 14, 2019
1. Solve $m^2 \equiv 1 \pmod{7}$
1. Solve $m^2 \equiv 1 \pmod{7}$ $m = 1, 6$
1. Solve \( m^2 \equiv 1 \pmod{7} \) \( m = 1, 6 \)
2. Solve \( m^2 \equiv 2 \pmod{7} \)

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

\( p-1 \) elements of \{1, \ldots, p-1\} 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.
1. Solve $m^2 \equiv 1 \pmod{7} \quad m = 1, 6$

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

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

\( p - 1 \) elements of \( \{1, \ldots, p-1\} \) 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.
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

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

$p-1/2$ elements of $\{1, \ldots, p-1\}$ 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.
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 \( m^2 \equiv 4 \pmod{7} \) \( m = 2, 5 \)

Since \( a^2 = (-a)^2 \) will always have, for all prime \( p \), \( p - 1 \) elements of \( \{1, \ldots, p-1\} \) have sqrts mod \( p \). \( p - 1 \) elements of \( \{1, \ldots, p-1\} \) 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.
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 $m^2 \equiv 1 \pmod{7}$ $m = 1, 6$

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
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

Since $a^2 = (-a)^2$ will always have, for all prime $p$, $p - 1$ elements of \{1, \ldots, p-1\} have sqrts mod $p$.
$p - 1$ elements of \{1, \ldots, p-1\} 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.
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 \(\{1, \ldots, p-1\}\) have sqrts mod $p$. \(\frac{p-1}{2}\) elements of \(\{1, \ldots, p-1\}\) 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!
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 \( m^2 \equiv 9 \) (mod 1147)
2. Solve \( m^2 \equiv 101 \) (mod 1147)
What about sqrt mod a composite. Try these:

1. Solve $m^2 \equiv 9 \pmod{1147}$
   - $m = 3, 1147 - 3 = 1144$. More?
2. Solve $m^2 \equiv 101 \pmod{1147}$
   - $m = \text{? Hmmm.}$

1. Solve $m^2 \equiv 9 \pmod{1147}$: $3, 1147 - 3 = 1144$ easy.
   - It turns out that $34^2 \equiv 9 \pmod{1147}$, hence $1147 - 34 = 1113$ also a sqrt of 9. How to find those?

Vote: Is finding sqrts mod $n$ hard? Yes, No, Unknown.

Unknown: Many comp. questions in Number Theory are Unknown.
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 $m^2 \equiv 9 \pmod{1147}$: $m = 3, 1147 - 3 = 1144$. More?
What about \( \text{sqrt} \) mod a composite. Try these:

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

1. Solve \( m^2 \equiv 9 \pmod{1147} \): \( m = 3, 1147 - 3 = 1144 \). More?
2. Solve \( m^2 \equiv 101 \pmod{1147} \):
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 $m^2 \equiv 9 \pmod{1147}$: $m = 3, \ 1147 - 3 = 1144$. More?
2. Solve $m^2 \equiv 101 \pmod{1147}$: $m =$? Hmmm.
What about sqrt mod a composite. Try these:

1. Solve \( m^2 \equiv 9 \pmod{1147} \)
   
   1. Solve \( m^2 \equiv 9 \pmod{1147} \): \( m = 3, 1147 - 3 = 1144 \). More?

2. Solve \( m^2 \equiv 101 \pmod{1147} \):
   
   2. Solve \( m^2 \equiv 101 \pmod{1147} \): \( m = ? \) Hmm.

Solve \( m^2 \equiv 9 \pmod{1147} \): 3, 1147 – 3 = 1144 easy.

It turns out that \( 34^2 \equiv 9 \pmod{1147} \), hence 1147 – 34 = 1113 also a sqrt of 9. How to find those?

**Vote:** Is finding sqrts mod \( N \) hard? Yes, No, Unknown.
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 $m^2 \equiv 9 \pmod{1147}$: $m = 3$, $1147 - 3 = 1144$. More?
2. Solve $m^2 \equiv 101 \pmod{1147}$: $m =$? Hmmm.

Solve $m^2 \equiv 9 \pmod{1147}$: 3, 1147 − 3 = 1144 easy.
It turns out that $34^2 \equiv 9 \pmod{1147}$, hence 1147 − 34 = 1113 also a sqrt of 9. How to find those?

**Vote:** Is finding sqrts mod $N$ hard? Yes, No, Unknown.

**Unknown:** Many comp. questions in Number Theory are Unknown.
\[ m^2 \equiv 101 \pmod{31 \times 37} \]

We first sqrt mod the factors:

\[ m^2 \equiv 101 \pmod{31}. \quad m^2 \equiv 8 \pmod{31}: \quad m \equiv \pm 15 \pmod{31} \]
\[ m^2 \equiv 101 \pmod{31 \times 37} \]

We first sqrt mod the factors:
\[ m^2 \equiv 101 \pmod{31}. \quad m^2 \equiv 8 \pmod{31}: \quad m \equiv \pm 15 \pmod{31} \]
\[ m^2 \equiv 101 \pmod{37}. \quad m^2 \equiv 27 \pmod{37} \quad m \equiv \pm 8 \pmod{37}. \]
\[ m^2 \equiv 101 \pmod{31 \times 37} \]

We first sqrt mod the factors:
\[ m^2 \equiv 101 \pmod{31}. \quad m^2 \equiv 8 \pmod{31}: \quad m \equiv \pm 15 \pmod{31} \]
\[ m^2 \equiv 101 \pmod{37}. \quad m^2 \equiv 27 \pmod{37} \quad m \equiv \pm 8 \pmod{37}. \]

One approach: Want number \( m \in \{1, \ldots, 1146\} \) such that
\[ m \equiv 15 \pmod{31} \]
\[ m \equiv 8 \pmod{37} \]
We first sqrt mod the factors:

\[ m^2 \equiv 101 \pmod{31 \times 37} \]

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

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

One approach: Want number \( m \in \{1, \ldots, 1146\} \) such that

\[ m \equiv 15 \pmod{31} \]

\[ m \equiv 8 \pmod{37} \]

Use Chinese Remainder Theorem to get:

\[ m = 15918 \equiv 1007 \pmod{1147} \]
By using $\pm 15 \ (\text{mod } 31)$ and $\pm 8 \ (\text{mod } 37)$ 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 $N = pq$.

Is finding sqrts mod $N$ (factors of $N$ not known) 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 $N = pq$.

Is finding sqrts mod $N$ (factors of $N$ not known) hard?

Normally I would say

Finding sqrt mod $N$ (factors of $N$ not known) thought 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 $N = pq$.

Is finding sqrts mod $N$ (factors of $N$ not known) hard?

Normally I would say

Finding sqrt mod $N$ (factors of $N$ not known) thought 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.
How hard is square roots mod $N$ when factors of $N$ not known?

**Theorem**: If finding square roots 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 square roots.
3. If it doesn’t have $\geq 4$ square roots then goto step 2.
4. The four square roots 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.
All you Need to Know for Rabin’s Scheme

1. Finding primes is easy.
2. Squaring is easy.
3. If $N$ is factored then $\sqrt{N} \mod N$ is easy.
4. If $N$ is not factored then $\sqrt{N} \mod N$ is thought to be hard (equiv to factoring).
Rabin’s Encryption Scheme

$L$ is a security parameter

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

$L$ is a security parameter

1. Alice gen $p, q$ primes of length $L$. Let $N = pq$. Send $N$.
2. Encode: To send $m$, Bob sends $c \equiv m^2 \pmod{N}$.
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

\( L \) is a security parameter

1. Alice gen \( p, q \) primes of length \( L \). Let \( N = pq \). Send \( N \).
2. Encode: To send \( m \), Bob sends \( c \equiv m^2 \pmod{N} \).
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? (in red)

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? (in red)

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.
How to Modify Rabin’s Encryption? (in red)

Let's look at mod 21 = 3 × 7.

1^2, 8^2, 13^2, 20^2 ≡ 1
2^2, 5^2, 16^2, 19^2 ≡ 4
3^2, 18^2 ≡ 9
4^2, 10^2, 11^2, 17^2 ≡ 16
6^2, 15^2 ≡ 15
7^2, 14^2 ≡ 7
9^2, 12^2 ≡ 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?
How to Modify Rabin’s Encryption? (in blue)

Let's 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
How to Modify Rabin’s Encryption? (in blue)

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.
How to Modify Rabin’s Encryption? (in blue)

Let’s look at mod \( 21 = 3 \times 7 \).
\[
\begin{align*}
1^2, \quad 8^2, \quad 13^2, \quad 20^2 &\equiv 1 \\
2^2, \quad 5^2, \quad 16^2, \quad 19^2 &\equiv 4 \\
3^2, \quad 18^2 &\equiv 9 \\
4^2, \quad 10^2, \quad 11^2, \quad 17^2 &\equiv 16 \\
6^2, \quad 15^2 &\equiv 15 \\
7^2, \quad 14^2 &\equiv 7 \\
9^2, \quad 12^2 &\equiv 18
\end{align*}
\]

**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

We use **Theorem** to modify Rabin Encryption.
Squares mod 77 (in red)

Squares: \{1, 4, 9, 14, 15, 16, 22, 25, 36, 42, 49, 64, 70, 71\}
\[
\sqrt{1} = 1, 34, 43, 76
\]
\[
\sqrt{4} = 2, 9, 68, 75
\]
\[
\sqrt{9} = 3, 25, 52, 74
\]
\[
\sqrt{14} = 28, 49
\]
\[
\sqrt{15} = 13, 20, 57, 64
\]
\[
\sqrt{16} = 4, 18, 59, 73
\]
\[
\sqrt{22} = 22, 55
\]
\[
\sqrt{25} = 5, 16, 61, 72
\]
\[
\sqrt{36} = 6, 27, 50, 71
\]
\[
\sqrt{42} = 14, 63
\]
\[
\sqrt{49} = 7, 70
\]
\[
\sqrt{64} = 8, 71
\]
\[
\sqrt{70} = 35, 42
\]
\[
\sqrt{71} = 15, 29, 48, 62
\]
Squares mod 77 (in blue)

Squares: \{1, 4, 9, 14, 15, 16, 22, 25, 36, 42, 49, 64, 70, 71\}
\sqrt{1} = 1, 34, 43, 76
\sqrt{4} = 2, 9, 68, 75
\sqrt{9} = 3, 25, 52, 74
\sqrt{14} = 28, 49
\sqrt{15} = 13, 20, 57, 64
\sqrt{16} = 4, 18, 59, 73
\sqrt{22} = 22, 55
\sqrt{25} = 5, 16, 61, 72
\sqrt{36} = 6, 27, 50, 71
\sqrt{42} = 14, 63
\sqrt{49} = 7, 70
\sqrt{64} = 8, 71
\sqrt{70} = 35, 42
\sqrt{71} = 15, 29, 48, 62
Rabin’s Enc Scheme 2.0—by Blum and Williams.

$L$ is a security parameter.

1. Alice gen $p, q$ primes of length $L$ 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 $SQ_N$. 
(You’ve seen this before but Good do see it again.)

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 $NSQ_N$. 
Another way To Make Rabin Unique

Recall Rabin’s Scheme:

$L$ is a security parameter

1. Alice gen $p, q$ primes of length $L$. 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?
Another way To Make Rabin Unique

Recall Rabin’s Scheme:
$L$ is a security parameter

1. Alice gen $p, q$ primes of length $L$. 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

$L$ is a security parameter

1. Alice gen $p, q$ primes of length $L$. Let $N = pq$. NEW: Let $x$ be a rand 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 $m^2 - cm + x = 0$. 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)

CON $m$ has to be invertible, so $m^{-1}$ exists. Is this bad?
If $m$ has to be invertible is that bad?
If $m$ has to be invertible is that bad?

Yes
If $m$ has to be invertible is that bad?

Yes

Recall To solve NY,NY problem have 2/3 of the message be the real message, and 1/3 be random pads.
If $m$ has to be invertible is that bad?

Yes

Recall To solve NY,NY problem have 2/3 of the message be the real message, and 1/3 be random pads.
Want to send $m$ (which is $2L/3$ bits).
Random $r$ of length $L/3$
Now send $rm$ (concat)
If $m$ has to be invertible is that bad?

Yes

Recall To solve NY,NY problem have 2/3 of the message be the real message, and 1/3 be random pads.
Want to send $m$ (which is $2L/3$ bits).
Random $r$ of length $L/3$
Now send $rm$ (concat)
We need to pick $r$ so that $rm$ is invertible.
If $m$ has to be invertible is that bad?

Yes

**Recall** To solve NY, NY problem have 2/3 of the message be the real message, and 1/3 be random pads. Want to send $m$ (which is $2L/3$ bits).
Random $r$ of length $L/3$
Now send $rm$ (concat)
We need to pick $r$ so that $rm$ is invertible.
Who needs the hassle?
Can Rabin’s Encryption Scheme Can Be Cracked?

$L$ is a security parameter

1. Alice gen $p, q$ primes of length $L$. Let $N = pq$. Send $N$.
2. Encode: To send $m$, Bob sends $c = m^2 \pmod{N}$.
3. Decode: Alice can find some $m$ such that $m^2 \equiv c \pmod{N}$.
   (There will be several possible $m$’s, she picks out one somehow.)

Vote: Crackable, Uncrackable, Unknown
Can Rabin’s Encryption Scheme Can Be Cracked?

$L$ is a security parameter

1. Alice gen $p, q$ primes of length $L$. Let $N = pq$. Send $N$.
2. Encode: To send $m$, Bob sends $c = m^2 \pmod{N}$.
3. Decode: Alice can find some $m$ such that $m^2 \equiv c \pmod{N}$.
   (There will be several possible $m$’s, she picks out one somehow.)

Vote: Crackable, Uncrackable, Unknown

Crackable:

Attack!: Eve picks an $m$ and tricks Bob into sending message $m$ via $m^2 \equiv c$. Eve is hoping that Alice will find another sqrt of $m^2$. Say Bob 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. 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.
Goldwasser-Micali Encryption

October 14, 2019
Math Needed For Goldwasser-Micali Encryption

(You’ve seen this before but Good do see it again.)

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 Goldwasser-Micali Encryption

1. Given $L$, can gen random primes of length $L$ easily.
2. Given $p, q$ let $N = pq$. Can gen a random $z \in NSQ_N$ 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!)
Goldwasser-Micali Encryption

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

1. Alice gen $p, q$ primes of length $L$, and $z \in NSQ_N$. Computes $N = pq$. Send $(N, z)$.

2. Encode: To send $m \in \{0, 1\}$, Bob picks random $x \in \mathbb{Z}_N$, 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.
Goldwasser-Micali Encryption Hardness Assumption

**SQ problem:** Given \((c, N)\) determine if \(c \in SQ_N\).

**Hardness Assumption:** 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 Goldwasser-Micali:

**BIGGEST CON** They take life one bit at a time. Really?
Math You Need For Blum-Goldwasser Encryption

(You have seen this before but want to get us all on the same page.)

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 most of this before but want to get us all on the same page.)

1. Given $L$, can gen random primes of length $L$ easily.
2. Given $p, q$ let $N = pq$. Can gen a random $z \in NSQ_N$ 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. More on that later.
7. $LSB(x)$ is the least significant bit of $x$. 
Blum-Goldwasser Enc. \( L \) Sec Param, \( M \) length of msg

1. Alice: \( p, q \) primes len \( L \), \( p, q \equiv 3 \pmod{4} \). \( N = pq \). Send \( N \).

2. Encode: Bob sends \( m \in \{0, 1\}^M \): picks random \( r \in \mathbb{Z}_N \)
   \( x_1 = r^2 \mod N \) \quad \( b_1 = \text{LSB}(x_1) \).
   \( x_2 = x_1^2 \mod N \) \quad \( b_2 = \text{LSB}(x_2) \).
   
   \vdots
   \( x_{M+1} = x_L^2 \mod N \) \quad \( b_{M+1} = \text{LSB}(x_{M+1}) \).
   Send \( c = ((m_1 \oplus b_1, \ldots, m_M \oplus b_M), x_{M+1}) \).

3. Decode: Alice: From \( x_{M+1} \) Alice can compute \( x_M, \ldots, x_1 \) by sqrt (can do since Alice has \( p, q \)). Then can compute \( b_1, \ldots, b_M \) and hence \( m_1, \ldots, m_M \).

**BIG PRO** Hardness assumption – next slide.

**TIME:** For \( L \) bits need \((L + 3) \log N\) steps. Better than Goldwasser-Micali.
The sequence $b_0, b_1, \ldots, b_L$ is the output of a known pseudorandom generator called BBS (Blum-Blum-Shub).

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

\textbf{Hardness Assumption (HA)} BBS is computationally hard.

\textbf{Natural?} Is the HA natural? Discuss. Vote.
The sequence $b_0, b_1, \ldots, b_L$ is the output of a known pseudorandom generator called BBS (Blum-Blum-Shub).

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

**Hardness Assumption (HA)** BBS is computationally hard.

**Natural?** Is the HA natural? Discuss. Vote.

**PRO** HA is equivalent to factoring being hard!