Misc Crypto
Using the Same $e$
HW 5 Prob 3
Advice for Alice When she uses RSA

Recall:
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

Using the Same $e$ Gets me nervous.
Bill vs Student; Theory vs Practice

Bill: Alice should not use the same value of $e$ all the time. If she does then that $e$ becomes an object of study. Saadiq finds a Muffin-connection to that $e$! Vince finds a reciprocal-connection to that $e$! Jacob finds a string-theory-connection to that $e$! etc.

Student: I've read on the web that you should use $e = 2^{2^4} + 1$, the fourth Fermat Prime. And the article 20 years of attacks on RSA (on the course website now) says so. The article was written by a theorist like you, Dan Boneh.

Bill: Dan Boneh is a much better theorist than me. Email me the website and paper and I'll see what's up. Well pierce my ears and call me drafty! In practice you SHOULD use $e = 2^{2^4} + 1$. 

Bill vs Student; Theory vs Practice

Bill: Alice should not use the same value of $e$ all the time. If she does then that $e$ becomes an object of study. Saadiq finds a Muffin-connection to that $e$! Vince finds a reciprocal-connection to that $e$! Jacob finds a string-theory-connection to that $e$! etc.

Student: I’ve read on the web that you should use $e = 2^{2^4} + 1$, the fourth Fermat Prime. And the article 20 years of attacks on RSA (on the course website now) says so. The article was written by a theorist like you, Dan Boneh.
Bill: Alice should not use the same value of $e$ all the time. If she does then that $e$ becomes an object of study. Saadiq finds a Muffin-connection to that $e$! Vince finds a reciprocal-connection to that $e$! Jacob finds a string-theory-connection to that $e$! etc.

Student: I’ve read on the web that you should use $e = 2^{2^4} + 1$, the fourth Fermat Prime. And the article *20 years of attacks on RSA* (on the course website now) says so. The article was written by a theorist like you, Dan Boneh.

Bill: Dan Boneh is a much better theorist than me. Email me the website and paper and I’ll see what’s up.
Bill: Alice should not use the same value of $e$ all the time. If she does then that $e$ becomes an object of study. Saadiq finds a Muffin-connection to that $e$! Vince finds a reciprocal-connection to that $e$! Jacob finds a string-theory-connection to that $e$! etc.

Student: I’ve read on the web that you should use $e = 2^{24} + 1$, the fourth Fermat Prime. And the article *20 years of attacks on RSA* (on the course website now) says so. The article was written by a theorist like you, Dan Boneh.

Bill: Dan Boneh is a much better theorist than me. Email me the website and paper and I’ll see what’s up. Well pierce my ears and call me drafty! In practice you SHOULD use $e = 2^{24} + 1$. 
Why $e = 2^{2^4} + 1$ is good to use

Recall that in RSA Bob must compute $m^e$.  

**Bill:** Can do $m^e$ with repeated squaring in roughly $\log_2(m)$ steps.  

**Practioner:** roughly $\log_2(m)$ steps? Let's see:  

$e = 2^{2^4} + 1$: You do the usual repeated squaring $m^2, m^2^2, m^2^3, \ldots, m^{2^{2^4}}$ in 16 steps. Total: 17 steps.  

$e = 2^{2^4} - 1$: You do the usual repeated squaring $m^2, m^2^2, m^2^3, \ldots, m^{2^{2^4} - 1}$ in 15 steps. Then 15 MORE mults. so roughly 30 steps.
Why $e = 2^{2^4} + 1$ is good to use

Recall that in RSA Bob must compute $m^e$.

Bill: Can do $m^e$ with repeated squaring in roughly $\log_2(m)$ steps.

Practioner: roughly $\log_2(m)$ steps? Let's see:

$e = 2^{2^4} + 1$: You do the usual repeated squaring

$m^2, m^2^2, m^2^3, \ldots, m^{2^{2^4}}$ in 16 steps. Total: 17 steps.

$e = 2^{2^4} - 1$: You do the usual repeated squaring

$m^2, m^2^2, m^2^3, \ldots, m^{2^{2^4}-1}$ in 15 steps. Then 15 MORE mults. so roughly 30 steps.

Bill: Does 16 vs 30 steps matter?
Why $e = 2^{2^4} + 1$ is good to use

Recall that in RSA Bob must compute $m^e$.

**Bill:** Can do $m^e$ with repeated squaring in roughly $\lg_2(m)$ steps.

**Practioner:** roughly $\lg_2(m)$ steps? Let’s see:

- $e = 2^{2^4} + 1$: You do the usual repeated squaring $m^2$, $m^{2^2}$, $m^{2^3}$, ..., $m^{2^{2^4}}$ in 16 steps. Total: 17 steps.

- $e = 2^{2^4} - 1$: You do the usual repeated squaring $m^2$, $m^{2^2}$, $m^{2^3}$, ..., $m^{2^{2^4}-1}$ in 15 steps. Then 15 MORE mults. so roughly 30 steps.

**Bill:** Does 16 vs 30 steps matter?

**Practioner:** YES you moron.
Why \( e = 2^{2^4} + 1 \) is good to use

Recall that in RSA Bob must compute \( m^e \).

**Bill:** Can do \( m^e \) with repeated squaring in roughly \( \log_2(m) \) steps.

**Practioner:** roughly \( \log_2(m) \) steps? Lets see:

\( e = 2^{2^4} + 1 \): You do the usual repeated squaring

\( m^2, m^2^2, m^2^3, \ldots, m^{2^{2^4}} \) in 16 steps. Total: 17 steps.

\( e = 2^{2^4} - 1 \): You do the usual repeated squaring

\( m^2, m^{2^2}, m^{2^3}, \ldots, m^{2^{2^4}-1} \) in 15 steps. Then 15 MORE mults. so roughly 30 steps.

**Bill:** Does 16 vs 30 steps matter?

**Practioner:** YES you moron.

**Bill:** Only Cheyenne is allowed to call me a moron.
$e = 2^{2^4} + 1$ vs my fears

In Practice: Want to use $e = 2^{2^4} + 1$ since:

1. Only 15 mults.
2. $2^{2^4} + 1$ is big enough to ward off the low-e attackes
3. $2^{2^4} + 1$ is prime, so only way it fails to be rel prime to $R = (p - 1)(q - 1)$. is if it divides $R$. Unlikely and easily tested.

In Theory: Do not want to use the same $e$ over and over again for fear of this being exploited.

Who is Right: $e = 2^{16} + 1$ is right.
\[ e = 2^{2^4} + 1 \] vs my fears

**In Practice:** Want to use \( e = 2^{2^4} + 1 \) since:

1. Only 15 mults.
2. \( 2^{2^4} + 1 \) is big enough to ward off the low-e attackes.
3. \( 2^{2^4} + 1 \) is prime, so only way it fails to be rel prime to \( R = (p - 1)(q - 1) \). is if it divides \( R \). Unlikely and easily tested.

**In Theory:** Do not want to use the same \( e \) over and over again for fear of this being exploited.

**Who is Right:** \( e = 2^{16} + 1 \) is right. For now
Vig Book Cipher
Vig Book Cipher

A student said

*What if the Vig cipher uses a book for the key?*
A student said

*What if the Vig cipher uses a book for the key?*

YES- people HAVE done this! Is it a good idea? *Discuss*
A student said

*What if the Vig cipher uses a book for the key?*

YES- people HAVE done this! Is it a good idea? **Discuss**

1. Before modern computer era: YES.
2. Now: NO.
How to Crack the Vig Book Cipher

Key: Both Key and Text have the English Lang Frequencies.
How to Crack the Vig Book Cipher

Eve sees a $d$. What does Eve know? Discuss
How to Crack the Vig Book Cipher

Eve sees a $d$. What does Eve know? Discuss

The following are the only possibilities for (letter in Key, Letter in Text)

$(a, d), (z, e), (y, f), (w, g), \ldots, (b, c)$

Only 26 possibilities. What of it? Discuss
How to Crack the Vig Book Cipher

Eve sees a $d$. What does Eve know? Discuss

The following are the only possibilities for (letter in Key, Letter in Text)

$(a, d), (z, e), (y, f), (w, g), \ldots, (b, c)$

Only 26 possibilities. What of it? Discuss

Some of the pairs are more likely than others.

1. $(z, e)$: Hmm, $z$ is unlikely but $e$ is likely.
2. $(a, d)$: Hmm, seems more likely than $(z, e)$.
3. Can rank which are more likely in a variety of ways.
4. Can then use adjacent letters and freq of adjacent pairs.

Note: For Real! Book-Vig-Cipher was used and was cracked.
Making Vig Harder to Crack
Usual Vig

Key: A word or phrase. Example: $\text{dog} = (3,14,6)$. Easy to remember and transmit.

Example using $\text{dog}$.
Shift 1st letter by 3
Shift 2nd letter by 14
Shift 3rd letter by 6
Shift 4th letter by 3
Shift 5th letter by 14
Shift 6th letter by 6, etc.

$\text{Jacob Prinz is a Physics Major}$

encrypts to

$\text{MOIRP VUWTC WYDDN BOFGS DXUU}$
Getting More Out of Your Phrase

If the key was

Corn Flake

You would get a key of length 9. We want More
If the key was Corn Flake, you would get a key of length 9. We want More. Corn is 4 letters long. Flake is 5 letters long. We form a key of length \( LCM(4, 5) = 20 \).

```
C O R N C O R N C O R N C O R N
F L A K E F L A K E F L A K E
```

ADD it up to get new 20-long key.

```
7 25 17 23 6 19 2 13 12 18 22 24 2 24 21 18 13
```

Wheel of Fortune would yield how long a key Discuss.
Getting More Out of Your Phrase

If the key was Corn Flake

You would get a key of length 9. We want More

Corn is 4 letters long. Flake is 5 letters long
We form a key of length \( LCM(4, 5) = 20 \).

\[
\begin{array}{cccccccccccccccc}
C & O & R & N & C & O & R & N & C & O & R & N & C & O & R & N & C \\
\end{array}
\]

ADD it up to get new 20-long key.

Wheel of Fortune would yield how long a key Discuss
\( LCM(5, 2, 7) = 70 \).
Can Eve Still Crack Vig?

Yes (in the modern era) but its harder because of longer key. In an older era this may have made Vig go from crackable to uncrackable. But today, Vig is always crackable. Famous last words...
Can Eve Still Crack Vig?

Yes (in the modern era) but its harder because of longer key.

In an older era this may have made Vig go from crackable to uncrackable.

But today, Vig is always crackable.

Famous last words....
More on the Matrix Cipher History
Recall the Matrix Cipher

\( n \) are security parameters.

1. Alice picks an \( n \times n \) invertible matrix \( A \) of elements of \( \mathbb{Z}_{26} \). \( n \) public, \( A \) private. Bob also gets \( A \) (so this is private key). Alice and Bob also both compute \( A^{-1} \).

2. To encrypt a text \( m \) break it up into blocks of size \( n \), so

\[
m = m_1, m_2, \ldots, m_N
\]

And form \( C = Am_1, Am_2, \ldots, Am_N \).

3. To decrypt a text \( C \) break it up into blocks of size \( n \), so

\[
C = C_1, C_2, \ldots, C_N
\]

And form \( m = A^{-1}C_1, A^{-1}C_2, \ldots, A^{-1}C_N \).
Lester Hill proposed the Matrix Cipher in 1929. Called *Hill Cipher*.

He suggested the following (though he didn’t use Alice and Bob)

Alice and Bob are going to use the Matrix Cipher.
Inverting a matrix is hard (in 1929).

**Idea:** Alice comes up with a matrix that is its own inverse! She gives it to Bob and Bob does not have to invert!
Is the idea Good, Bad, or Idiotic. **Discuss**
Origin and Idiocy

Lester Hill proposed the Matrix Cipher in 1929. Called *Hill Cipher*.

He suggested the following (though he didn’t use Alice and Bob)

Alice and Bob are going to use the Matrix Cipher. Inverting a matrix is hard (in 1929).

Idea: Alice comes up with a matrix that is its own inverse! She gives it to Bob and Bob does not have to invert!

Is the idea Good, Bad, or Idiotic. Discuss

1. In 1929, and not assuming Kerckhoff’s principle, Good
2. In $\geq 1945$ or assuming Kerckhoff’s principle, Idiotic
3. There was never a time it was just bad
More on the Matrix Cipher
Can We Do Better Than $O(26^{n^2})$?
Can crack in $O(26^{n^2})$

1. Input $C$, a coded text. Know $n$.
2. For EVERY $n \times n$ invertible matrix $A$ over $\mathbb{Z}_p$,
   2.1 Decode $C$ into $m$ using $A$.
   2.2 IF LOOKS-LIKE-ENGLISH($m$)=YES then STOP and output $m$. else goto next matrix $A$

Takes roughly $O(26^{n^2})$ steps.
Can we do better? VOTE.

1. YES
2. NO - and we can PROVE we can’t do better with ciphertext-only.
3. UNKNOWN TO SCIENCE if we can do better with ciphertext-only.
Can crack in $O(26^{n^2})$

1. Input $C$, a coded text. Know $n$.
2. For EVERY $n \times n$ invertible matrix $A$ over $\mathbb{Z}_p$,
   2.1 Decode $C$ into $m$ using $A$.
   2.2 IF LOOKS-LIKE-ENGLISH($m$)=YES then STOP and output $m$. else goto next matrix $A$

Takes roughly $O(26^{n^2})$ steps.
Can we do better? VOTE.

1. YES
2. NO - and we can PROVE we can’t do better with ciphertext-only.
3. UNKNOWN TO SCIENCE if we can do better with ciphertext-only.

YES- we can do $O(n26^n)$. 
Can crack in $O(n26^n)$

The attack in the last slide went through every Matrix. **Better Idea:** We take life one row at a time. **Example:** 3 matrix cipher. Decode Matrix $B$.

$$C = c_1c_2\cdots c_N \text{ each } c_i \text{ is 3-long}$$

Guess the first row of $B$. Say:

$$\begin{pmatrix} 1 & 1 & 7 \\ * & * & * \\ * & * & * \end{pmatrix}$$

Let $Bc_i = m_i$. Then $(1, 1, 7) \cdot t_i = m_i^1$ is first letter of $m_i$.

$$(m_1^1, m_2^1, m_3^1, \ldots, m_N^1)$$

is every third letter. Can do IS-ENGLISH on it.
Can crack in $O(n26^n)$

Eve knows that Alice and Bob decode with $n \times n$ Matrix $B$. Ciphertext is

$$C = c_1c_2 \cdots c_N$$

$$c_i = c_i^1 \cdots c_i^n$$

For $i = 1$ to $n$

For all $r \in \mathbb{Z}_{26}^n$ (guess that $r$ is $i$th row of $B$).

$$T = (r \cdot c_1, \ldots, r \cdot c_N) \text{ (Is every } i\text{th letter.)}$$

IF IS-ENGLISH($T$) = YES then $r_i = r$ and goto next $i$. Else goto the next $r$.

$B$ is

$$\begin{pmatrix}
\cdots & r_1 & \cdots \\
\vdots & \vdots & \vdots \\
\cdots & r_n & \cdots 
\end{pmatrix}$$

Takes roughly $O(n26^n)$ steps.
Important Lesson

Assume: $26^{80}$ time is big enough to thwart Eve.

1. If we think that best Eve can do is $O(26^{n^2})$ then we take $n = 9$, so Eve needs $O(26^{81})$.

2. If we think that best Eve can do is $O(n26^n)$ then we take $n = 80$, so Eve needs $O(80 \times 26^{80})$.

The $O(n \times 26^n)$ cracking does not show that Matrix Cipher is insecure, just that we have to pick parameters bigger than we had thought.
The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system.
2. Alice and Bob have a proof that it is uncrackable.
3. Eve Cracks it.
4. Lather, Rinse, Repeat.

Above attack on Matrix Cipher is a microcosm of this history.
The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system.
The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system.
2. Alice and Bob have a proof that it is uncrackable.
The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system.
2. Alice and Bob have a proof that it is uncrackable.
3. Eve Cracks it.

Above attack on Matrix Cipher is a microcosm of this history.
The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system.
2. Alice and Bob have a proof that it is uncrackable.
3. Eve Cracks it.
4. Lather, Rinse, Repeat.
The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system.
2. Alice and Bob have a proof that it is uncrackable.
3. Eve Cracks it.
4. Lather, Rinse, Repeat.

Above attack on Matrix Cipher is a microcosm of this history.
Random Bits
Paraphrase of a Piazza conversation

**Student:** You said that generating Random Bits is hard. Why?
How Hard is it to Generate Truly Random Bits?

Paraphrase of a Piazza conversation

Student: You said that generating Random Bits is hard. Why?

Bill: Truly Rand Bits are hard. How would you do it?
Paraphrase of a Piazza conversation

Student: You said that generating Random Bits is hard. Why?

Bill: Truly Rand Bits are hard. How would you do it?

Student: Just use the Random function in Java!
How Hard is it to Generate Truly Random Bits?

Paraphrase of a Piazza conversation

Student: You said that generating Random Bits is hard. Why?

Bill: Truly Rand Bits are hard. How would you do it?

Student: Just use the Random function in Java!

Bill: Okay. How do they do it, and is it Truly Random?
Paraphrase of a Piazza conversation

**Student:** You said that generating Random Bits is hard. Why?

**Bill:** *Truly* Rand Bits are hard. How would you do it?

**Student:** Just use the Random function in Java!

**Bill:** Okay. How do they do it, and is it *Truly* Random?

**Student:** Enlighten me as to how Java does it and why it does not work. You are truly the wisest of them all!
Paraphrase of a Piazza conversation

**Student:** You said that generating Random Bits is hard. Why?

**Bill:** *Truly* Rand Bits are hard. How would you do it?

**Student:** Just use the Random function in Java!

**Bill:** Okay. How do they do it, and is it *Truly* Random?

**Student:** Enlighten me as to how Java does it and why it does not work. You are truly the wisest of them all!

[That last line is fictional.]
Paraphrase of a Piazza conversation

**Student:** You said that generating Random Bits is hard. Why?

**Bill:** *Truly* Rand Bits are hard. How would you do it?

**Student:** Just use the Random function in Java!

**Bill:** Okay. How do they do it, and is it *Truly* Random?

**Student:** Enlighten me as to how Java does it and why it does not work. You are truly the wisest of them all!

[That last line is fictional.]

**Bill:** I will give an example!
Awesome Vig or Psuedo One Time Pad

\( A = 01, \, B = 02, \, \cdots \, Z = 26 \) (Not our usual since \( A = 01 \).

View each letter as a two-digit number mod 26.

Want a LONG sequence of 2-digit numbers \( k_1, \, k_2, \, \ldots \)

1. Will code \( m_1, \, m_2, \, \ldots \) by, for each digit adding mod 10.
   Example: If key is 12 38 and message is 29 23 then send
   \[
   \begin{array}{cc}
   12 & 38 \\
   29 & 23 \\
   \hline
   31 & 51
   \end{array}
   \]
   So send 31 51 (these do not correspond to letters, thats fine).

   \( (m_1 + k_1 \pmod{10}, \, m_2 + k_2 \pmod{10}, \ldots \)

2. Can view as either a Vig with a very long key OR as a 1-time pad. We view as Vig since not truly 1-time pad.

How to get a long random (looking?) sequence? Next slide.
Use Rec. $x_0, A, B, M$ is Short Private Key

(Example from "Cracking" a Random Number Generator by James Reed. Paper on Course Website.)

$x_0 = 2134, A = 4381, B = 7364, M = 8397.$

\[
\begin{align*}
    x_0 & = 2134 \text{ view as } 21, 34 \\
    x_{n+1} & = 4381x_n + 7364 \pmod{8397}
\end{align*}
\]
Example

\[ x_0 = 2134 \]
\[ x_1 = 2160 \]
\[ x_2 = 6905 \]
\[ x_3 = 3778 \]

They start with \( x_1 \).

If the document began with the word secret then encode:

<table>
<thead>
<tr>
<th>Text-Letter</th>
<th>S</th>
<th>E</th>
<th>C</th>
<th>R</th>
<th>E</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text-Digits</td>
<td>19</td>
<td>05</td>
<td>03</td>
<td>18</td>
<td>05</td>
<td>20</td>
</tr>
<tr>
<td>Key-Digits</td>
<td>21</td>
<td>60</td>
<td>69</td>
<td>05</td>
<td>37</td>
<td>78</td>
</tr>
<tr>
<td>Ciphertext</td>
<td>30</td>
<td>65</td>
<td>62</td>
<td>13</td>
<td>32</td>
<td>98</td>
</tr>
</tbody>
</table>
Example

Alice sends Bob a document using the $x_i$ as a Vig coding two chars at a time.

Eve knows rec of form $x_{n+1} = Ax_n + B \pmod{M}$.

Eve knows that $A, B, M$ are all 4-digits.
Example

Alice sends Bob a document using the $x_i$ as a Vig coding two chars at a time.

Eve knows rec of form $x_{n+1} = Ax_n + B \pmod{M}$.

Eve knows that $A, B, M$ are all 4-digits.

Eve knows that the document is about India and Pakistan.

Eve thinks Pakistan will be in the document.

<table>
<thead>
<tr>
<th>Text-Letter</th>
<th>P</th>
<th>A</th>
<th>K</th>
<th>I</th>
<th>S</th>
<th>T</th>
<th>A</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text-Digits</td>
<td>16</td>
<td>01</td>
<td>11</td>
<td>09</td>
<td>19</td>
<td>20</td>
<td>01</td>
<td>14</td>
</tr>
</tbody>
</table>
Eve can crack it!

Eve tries PAKISTAN on every sequence of 8 letters. We describe what tries means.

<table>
<thead>
<tr>
<th>Text-Letter</th>
<th>P</th>
<th>A</th>
<th>K</th>
<th>I</th>
<th>S</th>
<th>T</th>
<th>A</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text-Digits</td>
<td>16</td>
<td>01</td>
<td>11</td>
<td>09</td>
<td>19</td>
<td>20</td>
<td>01</td>
<td>14</td>
</tr>
<tr>
<td>Ciphertext</td>
<td>24</td>
<td>66</td>
<td>87</td>
<td>47</td>
<td>17</td>
<td>45</td>
<td>26</td>
<td>96</td>
</tr>
</tbody>
</table>

If Eve’s guess is correct then:

| Key–Digits | 18| 65| 76| 48| 08| 25| 25| 82 |

Since $x_{n+1} = Ax_n + B \pmod{M}$

7648 $\equiv$ 1865A + B \pmod{M}

825 $\equiv$ 7648A + B \pmod{M}

2582 $\equiv$ 825A + B \pmod{M}

Can we solve these? (The title Eve can crack it! gives it away!)
Eve can crack it!

EQ1: $7648 \equiv 1865A + B \pmod{M}$
EQ2: $825 \equiv 7648A + B \pmod{M}$
EQ3: $2582 \equiv 825A + B \pmod{M}$

By looking at EQ1−EQ2 and EQ2−EQ3 get 2 equations and no $B$
EQ4: $-6823 \equiv 5783A \pmod{M}$
EQ5: $-5066 \equiv -1040A \pmod{M}$

Mult EQ4 by 5066 and EQ5 by 6823 and subtract to get

$$-36, 392, 598 \equiv 0 \pmod{M}$$

Can we use this?
Eve can crack it!

EQ1: \[7648 \equiv 1865A + B \pmod{M}\]
EQ2: \[825 \equiv 7648A + B \pmod{M}\]
EQ3: \[2582 \equiv 825A + B \pmod{M}\]

By looking at EQ1–EQ2 and EQ2–EQ3 get 2 equations and no \(B\)
EQ4: \[-6823 \equiv 5783A \pmod{M}\]
EQ5: \[-5066 \equiv -1040A \pmod{M}\]

Mult EQ4 by 5066 and EQ5 by 6823 and subtract to get

\[-36, 392, 598 \equiv 0 \pmod{M}\]

Can we use this? Do chickens have lips!
Eve can crack it!

\[ 36, 392, 598 \equiv 0 \pmod{M} \]

\( M \) divides 36, 392, 598. Hence a SMALL number of possibilities for \( M \). Eve factors \( M \).

\[ 36, 392, 598 = 2 \times 3^3 \times 11 \times 197 \times 311 \]
Eve can crack it!

$$36, 392, 598 \equiv 0 \pmod{M}$$

$M$ divides $36, 392, 598$.
Hence a SMALL number of possibilities for $M$. Eve factors $M$.

$$36, 392, 598 = 2 \times 3^3 \times 11 \times 197 \times 311$$
Factoring? Really? Eve has to Factor?
Eve can crack it!

\[ 36, 392, 598 \equiv 0 \pmod{M} \]

\( M \) divides 36, 392, 598.
Hence a SMALL number of possibilities for \( M \). Eve factors \( M \).

\[ 36, 392, 598 = 2 \times 3^3 \times 11 \times 197 \times 311 \]
Factoring? Really? Eve has to Factor?
(Sarcastic) does she have a quantum computer?
Eve can crack it!

\[ 36, 392, 598 \equiv 0 \pmod{M} \]

\( M \) divides 36, 392, 598.

Hence a SMALL number of possibilities for \( M \). Eve factors \( M \).

\[ 36, 392, 598 = 2 \times 3^3 \times 11 \times 197 \times 311 \]

Factoring? Really? Eve has to Factor?

(Sarcastic) does she have a quantum computer?

Will come back to this.
Eve can crack it!

$$36, 392, 598 \equiv 0 \pmod{M}$$

$M$ divides 36, 392, 598. Hence a SMALL number of possibilities for $M$. Eve factors $M$.

$$36, 392, 598 = 2 \times 3^3 \times 11 \times 197 \times 311$$

Factoring? Really? Eve has to Factor? (Sarcastic) does she have a quantum computer?

Will come back to this.

1. $M$ is a divisor of 36, 392, 598
2. $M$ is 4 digits long
3. The cipher used 7648, so $M > 7648$

Only number that works is 8397.
Eve can crack it!

EQ4: $-6823 \equiv 5783A \pmod{M}$
EQ5: $-5066 \equiv -1040A \pmod{M}$
$M = 8397$

EQ4: $-6823 \equiv 5783A \pmod{8397}$
EQ5: $-5066 \equiv -1040A \pmod{8397}$
5783 has an inverse mod 8397 so can find $A$ from EQ4.

Find $A = 4381$

EQ1: $7648 \equiv 1865A + B \pmod{M}$
Use to find $B = 7364$.

If no solution then PAKISTAN was not there, try next spot.

Not done yet: use this to decode and see if it looks like English.
Eve allowed to factor?

Eve had to factor:

\[ 36, 392, 598 = 2 \times 3^3 \times 11 \times 197 \times 311 \]

We usually say

Factoring is Hard

Let's be careful there.

1. If Alice picks two primes \( p, q \) of length \( n \) and picks \( N = pq \) then factoring \( N \) is hard.

2. If Alice picks out a RANDOM number then half the time it's even. A third of the time is divided by 3. Not so hard to factor.

Our scenario is closer to RANDOM then to ALICE.
An Early Idea on Factoring
Jevons Number

In the 1870’s William Jevon’s wrote of the difficulty of factoring. We paraphrase Solomon Golomb’s Paraphrase:

*Jevons observed that there are many cases where an operation is easy but its inverse is hard. He mentioned encryption and decryption. He mentioned multiplication and factoring. He anticipated RSA!*

We now give a direct quote from Jevons

*Can the reader say what two numbers multiplied together will produce*

8, 616, 460, 799

*I think it is unlikely that anyone aside from myself will ever know.*
Jevons Number

\[ J = 8,616,460,799 \]

We can now factor \( J \) easily. Was Jevon’s comment stupid? Discuss
Jevons Number

\[ J = 8,616,460,799 \]

We can now factor \( J \) easily. Was Jevon’s comment stupid? Discuss

Jevons Number

\[ J = 8, 616, 460, 799 \]

We can now factor \( J \) easily. Was Jevon’s comment stupid? Discuss

2. Jevon’s did not predict computers. Should he have?
Jevons Number

\[ J = 8, 616, 460, 799 \]

We can now factor \( J \) easily. Was Jevon’s comment stupid? Discuss

2. Jevon’s did not predict computers. Should he have?
3. Jevon’s did not predict math would help. Should he have?
Jevons Number

\[ J = 8,616,460,799 \]

We can now factor \( J \) easily. Was Jevon’s comment stupid? Discuss

2. Jevon’s did not predict computers. Should he have?
3. Jevon’s did not predict math would help. Should he have?
4. Lehmer factored \( J \) in 1903 using Math and computation.
Jevons Number

\[ J = 8, 616, 460, 799 \]

We can now factor \( J \) easily. Was Jevon’s comment stupid? Discuss

2. Jevon’s did not predict computers. Should he have?
3. Jevon’s did not predict math would help. Should he have?
4. Lehmer factored \( J \) in 1903 using Math and computation.
5. Golomb in 1996 showed that, given the math of his day, Jevon’s number could be factored in reasonable time.
Jevons Number

\[ J = 8,616,460,799 \]

We can now factor \( J \) easily. Was Jevon’s comment stupid? Discuss

2. Jevon’s did not predict computers. Should he have?
3. Jevon’s did not predict math would help. Should he have?
4. Lehmer factored \( J \) in 1903 using Math and computation.
5. Golomb in 1996 showed that, given the math of his day, Jevon’s number could be factored in reasonable time.
6. Student: Why didn’t Jevon’s just Google Factoring Quickly
Jevons Number

\[ J = 8,616,460,799 \]

We can now factor \( J \) easily. Was Jevon’s comment stupid? Discuss

2. Jevon’s did not predict computers. Should he have?
3. Jevon’s did not predict math would help. Should he have?
4. Lehmer factored \( J \) in 1903 using Math and computation.
5. Golomb in 1996 showed that, given the math of his day, Jevon’s number could be factored in reasonable time.
6. Student: Why didn’t Jevon’s just Google Factoring Quickly
   Bill: They didn’t have the Web back then. Or Google.
Jevons Number

\[ J = 8,616,460,799 \]

We can now factor \( J \) easily. Was Jevon’s comment stupid? Discuss

2. Jevon’s did not predict computers. Should he have?
3. Jevon’s did not predict math would help. Should he have?
4. Lehmer factored \( J \) in 1903 using Math and computation.
5. Golomb in 1996 showed that, given the math of his day, Jevon’s number could be factored in reasonable time.
6. Student: Why didn’t Jevon’s just Google Factoring Quickly
   Bill: They didn’t have the Web back then. Or Google.
   Student: How did they live?
Jevons Number

\[ J = 8,616,460,799 \]

We can now factor \( J \) easily. Was Jevon’s comment stupid? Discuss

2. Jevon’s did not predict computers. Should he have?
3. Jevon’s did not predict math would help. Should he have?
4. Lehmer factored \( J \) in 1903 using Math and computation.
5. Golomb in 1996 showed that, given the math of his day, Jevon’s number could be factored in reasonable time.
6. **Student:** Why didn’t Jevon’s just Google **Factoring Quickly**
   **Bill:** They didn’t have the Web back then. Or Google.
   **Student:** How did they live?
   **Bill:** How indeed!
Golomb’s Method to Factor Jevons Number

\[ J = 8, 616, 460, 799 \]

We apply a method of Fermat (in the 1600’s) to the problem of factoring \( J \).

To factor \( J \) find \( x, y \) such that

\[ J = x^2 - y^2 = (x - y)(x + y) \]

So we must narrow our search for \( x, y \).
Golomb’s Method to Factor Jevons Number

\[ J = 8, 616, 460, 799 \]
\[ J = x^2 - y^2 \]
\[ x^2 - J = y^2 \]
\[ x^2 - J \equiv y^2 \pmod{100} \]

Since \( J \equiv 99, -J \equiv 1 \), so we have

\[ x^2 + 1 \equiv y^2 \pmod{100} \]
\[ x^2 + 1 \equiv y^2 \pmod{100} \]

All squares mod 100:

\[ \{00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49\} \cup \{56, 61, 64, 69, 76, 81, 84, 89, 96\} \]

The only pairs which differ by 1 are

(00, 01) and (24, 25). So either:

1. \( x^2 \equiv 0 \), so \( x \pmod{100} \in \{10, 20, 30, 40, 50, 60, 70, 80, 90\} \)
2. \( x^2 \equiv 24 \), so \( x \pmod{100} \in \{18, 32, 68, 82\} \)
Golomb Works Mod 1000

\[ x^2 - J \equiv y^2 \pmod{1000} \]

\[ x^2 + 201 \equiv y^2 \pmod{1000} \]

If \( x \pmod{100} \in \{10, 20, 30, 40, 50, 60, 70, 80, 90\} \) then \( x = 100a + 10b \)

\[ (100a + 10b)^2 + 201 \equiv y^2 \pmod{1000} \]

\[ 100b^2 + 201 \equiv y^2 \pmod{1000} \]

\( b \equiv 1 \pmod{2} \implies 100b^2 + 201 \notin SQ_{1000}, \) so \( b \equiv 0 \pmod{2} \).

1. \( x^2 \equiv 0, \) so \( x \pmod{100} \in \{20, 40, 60, 80\} \)
2. \( x^2 \equiv 24, \) so \( x \pmod{100} \in \{18, 32, 68, 82\} \)
Recap

Combine the two sets for $x \pmod{100}$ to get

$$x \pmod{100} \in \{18, 20, 32, 40, 60, 68, 80, 82\}$$

Since $J = x^2 - y^2$, $x^2 = J + y^2$, so

$$x \geq \left\lfloor \sqrt{J} \right\rfloor = 92824$$

Since $J = x^2 - y^2$, $x^2 - J = y^2$, hence

$$x^2 - J = y^2 \in SQ$$
Golomb’s Method to Factor Jevons Number: $x^2 \geq J$

1. $x \pmod{100} \in \{18, 20, 32, 40, 60, 68, 80, 82\}$
2. $x \geq \left\lfloor \sqrt{J} \right\rfloor = 92824$
3. $x^2 - J = y^2 \in SQ$

<table>
<thead>
<tr>
<th>x</th>
<th>y = $(x^2 - J)^{1/2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>92832</td>
<td>1148.6…</td>
</tr>
<tr>
<td>92840</td>
<td>1674.7…</td>
</tr>
<tr>
<td>92860</td>
<td>2553.1…</td>
</tr>
<tr>
<td>92868</td>
<td>2329.2…</td>
</tr>
<tr>
<td>92880</td>
<td>3199</td>
</tr>
</tbody>
</table>

AH-HA! We take $x = 92880$, $y = 3199$.

$92880^2 - 3199^2 = 8,616,460,799$

$(92880 - 3199)(92880 + 3199) = 8,616,460,799$

$(89681)(96079) = 8,616,460,799$