Yet Another RSA attack

October 7, 2019

RSA

Let L be a security parameter

1. Alice picks two primes p, q of length L 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

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

Review of RSA Attacks

1. If same e, $e \le L$. Low-e attack. Response Large e.
2. If same e, $m^e < N_1 \cdots N_L$. Low-e attack. Response Pad m.
3. NY,NY problem. Leaks info. Response Rand Pad m
4. Timing Attacks Response Rand Pad time.

Note items 1 and 2:

$$e \text{ same but } N\text{'s Different}$$

How about

$$N \text{ same but } e\text{'s Different}$$

Surely that can't be a problem!

Review of RSA Attacks

1. If same e, $e \le L$. Low-e attack. Response Large e.
2. If same e, $m^e < N_1 \cdots N_L$. Low-e attack. Response Pad m.
3. NY,NY problem. Leaks info. Response Rand Pad m
4. Timing Attacks Response Rand Pad time.

Note items 1 and 2:

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 same e, $e \le L$. Low-e attack. Response Large e.
2. If same e, $m^e < N_1 \cdots N_L$. Low-e attack. Response Pad m.
3. NY,NY problem. Leaks info. Response Rand Pad m
4. Timing Attacks Response Rand Pad time.

Note items 1 and 2:

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.

For this Attack $\equiv$ means $\equiv \pmod{N}$

For this Attack $\equiv$ **means** $\equiv \pmod{N}$

Same N, Rel Prime e's, 2 People. Example

1. Zelda is sending messages to Alice using $(1147, 341)$
2. Zelda is sending messages to Bob using $(1147, 408)$
3. Note that 341 and 408 are relatively prime. Bad idea?

Zelda sends m to both Alice and Bob. Eve sees

1. $m^{341} \pmod{1147}$
2. $m^{408} \pmod{1147}$

341 and 408 are rel prime

341, 407 are relatively prime. Lets find combo that adds to 1.
$408 = 1 \times 341 + 67$
$341 = 67 \times 5 + 6$
$67 = 6 \times 11 + 1$

$$1 = 67 - 6 \times 11 = 67 - (341 - 67 \times 5) \times 11 = 56 \times 67 - 11 \times 341$$

$$= 56 \times (408 - 341) - 11 \times 341 = 56 \times 408 - 67 \times 341$$

$$1 = 56 \times 408 - 67 \times 341$$

Example Continued

1. Zelda & Alice use: $(1147, 341)$. Zelda & Bob use $(1147, 408)$.
2. Zelda sends m to Alice via $m^{341} \pmod{1147}$.
3. Zelda sends m to Bob via $m^{408} \pmod{1147}$.
4. $1 = 56 \times 408 - 67 \times 341$

Example Continued

1. Zelda & Alice use: $(1147, 341)$. Zelda & Bob use $(1147, 408)$.
2. Zelda sends m to Alice via $m^{341} \pmod{1147}$.
3. Zelda sends m to Bob via $m^{408} \pmod{1147}$.
4. $1 = 56 \times 408 - 67 \times 341$

Eve does the following:

- Find inverse of m^{341} mod 1147. We call this m^{-341}.

Example Continued

1. Zelda & Alice use: $(1147, 341)$. Zelda & Bob use $(1147, 408)$.
2. Zelda sends m to Alice via $m^{341} \pmod{1147}$.
3. Zelda sends m to Bob via $m^{408} \pmod{1147}$.
4. $1 = 56 \times 408 - 67 \times 341$

Eve does the following:

- Find inverse of m^{341} mod 1147. We call this m^{-341}.
- Compute mod 1147:

$$(m^{408})^{56} \times (m^{-341})^{67} \equiv m^{56 \times 408 - 67 \times 341} \equiv m^1 \equiv m$$

Example Continued

1. Zelda & Alice use: $(1147, 341)$. Zelda & Bob use $(1147, 408)$.
2. Zelda sends m to Alice via $m^{341} \pmod{1147}$.
3. Zelda sends m to Bob via $m^{408} \pmod{1147}$.
4. $1 = 56 \times 408 - 67 \times 341$

Eve does the following:

- Find inverse of m^{341} mod 1147. We call this m^{-341}.
- Compute mod 1147:

$$(m^{408})^{56} \times (m^{-341})^{67} \equiv m^{56 \times 408 - 67 \times 341} \equiv m^1 \equiv m$$

Wow! Eve found m without factoring.

Same N, Rel Prime e's, 3 People. Example

1. Zelda is sending messages to Alice using $(1147, 35)$
2. Zelda is sending messages to Bob using $(1147, 100)$
3. Zelda is sending messages to Carol using $(1147, 126)$

Same N, Rel Prime e's, 3 People. Example

1. Zelda is sending messages to Alice using $(1147, 35)$
2. Zelda is sending messages to Bob using $(1147, 100)$
3. Zelda is sending messages to Carol using $(1147, 126)$

If some pair was rel prime then can use prior slide technique.

Same N, Rel Prime e's, 3 People. Example

1. Zelda is sending messages to Alice using $(1147, 35)$
2. Zelda is sending messages to Bob using $(1147, 100)$
3. Zelda is sending messages to Carol using $(1147, 126)$

If some pair was rel prime then can use prior slide technique.

$$35 = 5 \times 7 \qquad 100 = 2^2 \times 5^2 \qquad 126 = 2 \times 3^2 \times 7$$

Same N, Rel Prime e's, 3 People. Example

1. Zelda is sending messages to Alice using $(1147, 35)$
2. Zelda is sending messages to Bob using $(1147, 100)$
3. Zelda is sending messages to Carol using $(1147, 126)$

If some pair was rel prime then can use prior slide technique.

$$35 = 5 \times 7 \qquad 100 = 2^2 \times 5^2 \qquad 126 = 2 \times 3^2 \times 7$$

No pair is rel prime. Must be safe, right?

Same N, Rel Prime e's, 3 People. Example

1. Zelda is sending messages to Alice using $(1147, 35)$
2. Zelda is sending messages to Bob using $(1147, 100)$
3. Zelda is sending messages to Carol using $(1147, 126)$

If some pair was rel prime then can use prior slide technique.

$$35 = 5 \times 7 \qquad 100 = 2^2 \times 5^2 \qquad 126 = 2 \times 3^2 \times 7$$

No pair is rel prime. Must be safe, right? Wrong.

Same N, Rel Prime e's, 3 People. Example

1. Zelda is sending messages to Alice using $(1147, 35)$
2. Zelda is sending messages to Bob using $(1147, 100)$
3. Zelda is sending messages to Carol using $(1147, 126)$

If some pair was rel prime then can use prior slide technique.

$$35 = 5 \times 7 \qquad 100 = 2^2 \times 5^2 \qquad 126 = 2 \times 3^2 \times 7$$

No pair is rel prime. Must be safe, right? Wrong.

Definition A set of numbers is relatively prime if no number divides all of them. (We have so far just used sets of size 2.)

Same N, Rel Prime e's, 3 People. Example

1. Zelda is sending messages to Alice using $(1147, 35)$
2. Zelda is sending messages to Bob using $(1147, 100)$
3. Zelda is sending messages to Carol using $(1147, 126)$

If some pair was rel prime then can use prior slide technique.

$$35 = 5 \times 7 \qquad 100 = 2^2 \times 5^2 \qquad 126 = 2 \times 3^2 \times 7$$

No pair is rel prime. Must be safe, right? Wrong.

Definition A set of numbers is relatively prime if no number divides all of them. (We have so far just used sets of size 2.)

Theorem If a, b, c are rel prime then there exists x_1, x_2, x_3 such that $ax_1 + bx_2 + cx_3 = 1$.

Same N, Rel Prime e's, 3 People. Example

1. Zelda is sending messages to Alice using $(1147, 35)$
2. Zelda is sending messages to Bob using $(1147, 100)$
3. Zelda is sending messages to Carol using $(1147, 126)$

If some pair was rel prime then can use prior slide technique.

$$35 = 5 \times 7 \qquad 100 = 2^2 \times 5^2 \qquad 126 = 2 \times 3^2 \times 7$$

No pair is rel prime. Must be safe, right? Wrong.

Definition A set of numbers is relatively prime if no number divides all of them. (We have so far just used sets of size 2.)
Theorem If a, b, c are rel prime then there exists x_1, x_2, x_3 such that $ax_1 + bx_2 + cx_3 = 1$.

Example $27 \times 35 - 17 \times 100 + 6 \times 126 = 1$

Example Continued

Zelda sends m to both Alice and Bob. Eve sees

1. $m^{35} \pmod{1147}$
2. $m^{100} \pmod{1147}$
3. $m^{126} \pmod{1147}$

Example Continued

Zelda sends m to both Alice and Bob. Eve sees

1. $m^{35} \pmod{1147}$
2. $m^{100} \pmod{1147}$
3. $m^{126} \pmod{1147}$

Recall: $27 \times 35 - 17 \times 100 + 6 \times 126 = 1$

Example Continued

Zelda sends m to both Alice and Bob. Eve sees

1. $m^{35} \pmod{1147}$
2. $m^{100} \pmod{1147}$
3. $m^{126} \pmod{1147}$

Recall: $27 \times 35 - 17 \times 100 + 6 \times 126 = 1$

Eve does the following:

- Find inverse of m^{100} mod 1147. We call this m^{-100}.

Example Continued

Zelda sends m to both Alice and Bob. Eve sees

1. $m^{35} \pmod{1147}$
2. $m^{100} \pmod{1147}$
3. $m^{126} \pmod{1147}$

Recall: $27 \times 35 - 17 \times 100 + 6 \times 126 = 1$

Eve does the following:

- Find inverse of m^{100} mod 1147. We call this m^{-100}.
- Compute mod 1147:

$$(m^{35})^{27} \times (m^{-100})^{17} \times (m^{126})^{6} \equiv m^{27 \times 35 - 17 \times 100 + 6 \times 126} \equiv m^1 \equiv m$$

Wow! Eve found m without factoring.

Same N, Rel Prime e's, 2 People. General

1. Zelda is sending messages to Alice using (N, e_1)
2. Zelda is sending messages to Bob using (N, e_2)
3. e_1, e_2 are rel prime (Bad idea!).

Zelda sends m to both Alice, Bob, and Carol. Eve sees

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

Same N, Rel Prime e's, 2 People. General

1. Zelda is sending messages to Alice using (N, e_1)
2. Zelda is sending messages to Bob using (N, e_2)
3. e_1, e_2 are rel prime (Bad idea!).

Zelda sends m to both Alice, Bob, and Carol. Eve sees

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

e_1, e_2 rel prime, so find $x_1, x_2 \in \mathbb{Z}$: $e_1x_1 + e_2x_2 = 1$.

Same N, Rel Prime e's, 2 People. General

1. Zelda is sending messages to Alice using (N, e_1)
2. Zelda is sending messages to Bob using (N, e_2)
3. e_1, e_2 are rel prime (Bad idea!).

Zelda sends m to both Alice, Bob, and Carol. Eve sees

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

e_1, e_2 rel prime, so find $x_1, x_2 \in \mathbb{Z}$: $e_1 x_1 + e_2 x_2 = 1$.

$$(m^{e_1})^{x_1} \times (m^{e_2})^{x_2} \equiv m^{e_1 x_1 + e_2 x_2} \equiv m^1 \equiv m \pmod{N}$$

Same N, Rel Prime e's, 2 People. General

1. Zelda is sending messages to Alice using (N, e_1)
2. Zelda is sending messages to Bob using (N, e_2)
3. e_1, e_2 are rel prime (Bad idea!).

Zelda sends m to both Alice, Bob, and Carol. Eve sees

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

e_1, e_2 rel prime, so find $x_1, x_2 \in \mathbb{Z}$: $e_1x_1 + e_2x_2 = 1$.

$$(m^{e_1})^{x_1} \times (m^{e_2})^{x_2} \equiv m^{e_1x_1+e_2x_2} \equiv m^1 \equiv m \pmod{N}$$

Caveat if $x_i < 0$ need m^{e_i} to have inverse mod N.

Same N, Rel Prime e's, 2 People. General

1. Zelda is sending messages to Alice using (N, e_1)
2. Zelda is sending messages to Bob using (N, e_2)
3. e_1, e_2 are rel prime (Bad idea!).

Zelda sends m to both Alice, Bob, and Carol. Eve sees

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

e_1, e_2 rel prime, so find $x_1, x_2 \in \mathbb{Z}$: $e_1x_1 + e_2x_2 = 1$.

$$(m^{e_1})^{x_1} \times (m^{e_2})^{x_2} \equiv m^{e_1x_1+e_2x_2} \equiv m^1 \equiv m \pmod{N}$$

Caveat if $x_i < 0$ need m^{e_i} to have inverse mod N.
Wow Eve found m without factoring N.

Recap of What We've Done So Far

We did

1. Concrete example with Zelda sending to 2 people.
2. Concrete example with Zelda sending to 3 people.
3. General case with Zelda sending to 2 people.

We did not do

1. General case with Zelda Sending to 3 people.
2. General case with Zelda Sending to L people.

Work on the L-case is with your neighbor.

Same N, Rel Prime e's, L People. General

1. Zelda is sending messages to A_i using (N, e_i)
2. $e_1, \ldots, e_L$ are rel prime (Bad idea!).

Zelda sends m to $A_1, \ldots, A_L$. Eve sees, for $1 \le i \le L$, $m^{e_i} \pmod{N}$.

Same N, Rel Prime e's, L People. General

1. Zelda is sending messages to A_i using (N, e_i)
2. $e_1, \ldots, e_L$ are rel prime (Bad idea!).

Zelda sends m to $A_1, \ldots, A_L$. Eve sees, for $1 \le i \le L$, m^{e_i} (mod N).
$e_1, \ldots, e_L$ rel prime, so $\exists\ x_1, \ldots, x_L \in \mathbb{Z}$, $\sum_{i=1}^{n} e_i x_i = 1$.

Same N, Rel Prime e's, L People. General

1. Zelda is sending messages to A_i using (N, e_i)
2. $e_1, \ldots, e_L$ are rel prime (Bad idea!).

Zelda sends m to $A_1, \ldots, A_L$. Eve sees, for $1 \le i \le L$, $m^{e_i} \pmod{N}$.
$e_1, \ldots, e_L$ rel prime, so $\exists\ x_1, \ldots, x_L \in \mathbb{Z}$, $\sum_{i=1}^{n} e_i x_i = 1$. Eve finds $x_1, \ldots, x_L$ and then computes

$$(m^{e_1})^{x_1} \times \cdots \times (m^{e_L})^{x_L} \equiv m^{\sum_{i=1}^{n} e_i x_i} \equiv m^1 \equiv m \pmod{N}.$$

Same N, Rel Prime e's, L People. General

1. Zelda is sending messages to A_i using (N, e_i)
2. $e_1, \ldots, e_L$ are rel prime (Bad idea!).

Zelda sends m to $A_1, \ldots, A_L$. Eve sees, for $1 \le i \le L$, $m^{e_i} \pmod{N}$.
$e_1, \ldots, e_L$ rel prime, so $\exists\ x_1, \ldots, x_L \in \mathbb{Z}$, $\sum_{i=1}^{n} e_i x_i = 1$. Eve finds $x_1, \ldots, x_L$ and then computes

$$(m^{e_1})^{x_1} \times \cdots \times (m^{e_L})^{x_L} \equiv m^{\sum_{i=1}^{n} e_i x_i} \equiv m^1 \equiv m \pmod{N}.$$

Caveat if $x_i < 0$ need m^{e_i} to have inverse mod N.

Same N, Rel Prime e's, L People. General

1. Zelda is sending messages to A_i using (N, e_i)
2. $e_1, \ldots, e_L$ are rel prime (Bad idea!).

Zelda sends m to $A_1, \ldots, A_L$. Eve sees, for $1 \le i \le L$, $m^{e_i} \pmod{N}$.
$e_1, \ldots, e_L$ rel prime, so $\exists\ x_1, \ldots, x_L \in \mathbb{Z}$, $\sum_{i=1}^{n} e_i x_i = 1$. Eve finds $x_1, \ldots, x_L$ and then computes

$$(m^{e_1})^{x_1} \times \cdots \times (m^{e_L})^{x_L} \equiv m^{\sum_{i=1}^{n} e_i x_i} \equiv m^1 \equiv m \pmod{N}.$$

Caveat if $x_i < 0$ need m^{e_i} to have inverse mod N.
Big Caveat How to find $x_1, \ldots, x_L$? (Next Slide)

Same N, Rel Prime e's, L People. General

1. Zelda is sending messages to A_i using (N, e_i)
2. $e_1, \ldots, e_L$ are rel prime (Bad idea!).

Zelda sends m to $A_1, \ldots, A_L$. Eve sees, for $1 \le i \le L$, $m^{e_i} \pmod{N}$.
$e_1, \ldots, e_L$ rel prime, so $\exists\ x_1, \ldots, x_L \in \mathbb{Z}$, $\sum_{i=1}^{n} e_i x_i = 1$. Eve finds $x_1, \ldots, x_L$ and then computes

$$(m^{e_1})^{x_1} \times \cdots \times (m^{e_L})^{x_L} \equiv m^{\sum_{i=1}^{n} e_i x_i} \equiv m^1 \equiv m \pmod{N}.$$

Caveat if $x_i < 0$ need m^{e_i} to have inverse mod N.
Big Caveat How to find $x_1, \ldots, x_L$? (Next Slide)
Wow Eve found m without factoring N.

Finding $x_1, \ldots, x_L$

Problem Given $e_1, \ldots, e_L$ rel prime, find $x_1, \ldots, x_L \in \mathbb{Z}$ such that $\sum_{i=1}^{L} x_i e_i = 1$.

Finding $x_1, \ldots, x_L$

Problem Given $e_1, \ldots, e_L$ rel prime, find $x_1, \ldots, x_L \in \mathbb{Z}$ such that $\sum_{i=1}^{L} x_i e_i = 1$.

Your thoughts on this?

Finding $x_1, \ldots, x_L$

Problem Given $e_1, \ldots, e_L$ rel prime, find $x_1, \ldots, x_L \in \mathbb{Z}$ such that $\sum_{i=1}^{L} x_i e_i = 1$.

Your thoughts on this?

What you should be thinking Bill, do an example!

An Example

Recall If a, b rel prime then exists x_1, x_2, $ax_1 + bx_2 = 1$.

Generalized Let $d = \mathrm{GCD}(a, b)$. Then exists x_1, x_2, $ax_1 + bx_2 = d$.

Good News Euclidean Alg finds $d, x_1, x_2 y$.

An Example

Recall If a, b rel prime then exists x_1, x_2, $ax_1 + bx_2 = 1$.
Generalized Let $d = \mathrm{GCD}(a, b)$. Then exists x_1, x_2, $ax_1 + bx_2 = d$.
Good News Euclidean Alg finds $d, x_1, x_2 y$.
35, 100, 126.

1. Find x_1, x_2 such that $35x_1 + 100x_2 = 5$ (5 is GCD of 35 and 100)

$$35 \times 3 - 100 = 5$$

2. Find y_1, y_2 such that $5y_1 + 126y_2 = 1$

$$-25 \times 5 + 126 = 1$$

3.

$$-25 \times (35 \times 3 - 100) + 126 = 1$$

$$-75 \times 35 + 25 \times 100 + 1 \times 126 = 1$$

Note This is diff sol then got earlier. There are many solutions.

Algorithm for x_1, x_2, x_3

1. Input e_1, e_2, e_3
2. Find y_1, y_2 such that $e_1 y_1 + e_2 y_2 = d$ where $d = \mathrm{GCD}(e_1, e_2)$.
3. Find z_1, z_2 such that $dz_1 + e_3 z_2 = 1$.
4. $$dz_1 + e_3 z_2 = 1$$
$$(e_1 y_1 + e_2 y_2) z_1 + e_3 z_2 = 1$$
$$e_1 (y_1 z_1) + e_2 (y_2 z_1) + e_3 z_2 = 1$$
5. $x_1 = y_1 z_1$, $x_2 = y_2 z_1$, $x_3 = z_2$

Note Leave general case to the reader.

Advice for Zelda When she uses RSA

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

1. Either e_i's different or if all are e, then e large.
2. If all the e's are the same, pad m so m^e large.
3. Either N_i different or if all are N, e_i's not rel prime.
4. Randomly pad m for NY,NY problem.
5. Randomly pad time to ward of timing attacks.

Another Attack: Factoring Algorithms

October 7, 2019

Factoring Algorithm Ground Rules

- We only consider algorithms that, given N, find a non-trivial factor of N.
- We measure the run time as a function of $\lg N$ which is the *length* of the input. We may use L for this.
- We count $+$, $-$, $\times$, $\div$ as ONE step. A more refined analysis would count them as $(\lg x)^2$ steps where x is larger number you are dealing with.
- We leave out the O-of but always mean O-of
- We leave out the *expected time* but always mean it. Our algorithms are randomized.
- I will just give one factoring algorithm now since its point is more advice for Alice and Bob. Will give others later.

Multiplication HS Algorithm is $\lg x^2$ time. Tell Kolmogorov story.

Easy Factoring Algorithm

1. Input(N)
2. For $x = 2$ to $\lfloor N^{1/2} \rfloor$
   If x divides N then return x (and jump out of loop!).

This takes time $N^{1/2} = 2^{L/2}$.

Easy Factoring Algorithm

1. Input(N)
2. For $x = 2$ to $\lfloor N^{1/2} \rfloor$

   If x divides N then return x (and jump out of loop!).

This takes time $N^{1/2} = 2^{L/2}$.

Goal Do much better than time $N^{1/2}$.

Pollard's $p - 1$ Algorithm for Factoring (1974)

October 7, 2019

An Example That Does Not Quite Work

Want to factor 11227.
If p is a prime factor of 11227

1. p divides 11227
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm)
3. So $\mathrm{GCD}(2^{p-1} - 1, 11227)$ divides 11227.
4. So $\mathrm{GCD}(2^{p-1} - 1 \bmod 11227, 11227)$ divides 11227.

Lets find $\mathrm{GCD}(2^{p-1} - 1 \bmod 11227, 11227)$. Good idea?

An Example That Does Not Quite Work

Want to factor 11227.
If p is a prime factor of 11227

1. p divides 11227
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm)
3. So $\mathrm{GCD}(2^{p-1} - 1, 11227)$ divides 11227.
4. So $\mathrm{GCD}(2^{p-1} - 1 \bmod 11227, 11227)$ divides 11227.

Lets find $\mathrm{GCD}(2^{p-1} - 1 \bmod 11227, 11227)$. Good idea?

We do not know p :-(If we did know p we would be done.

Making the Example Work

Want to factor 11227.
If p is a prime factor of 11227. We do not know p.

1. p divides 11227
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm)
3. p divides $2^{k(p-1)} - 1 \bmod 11227$ for any k
4. Raise 2 to a power that we hope has $p - 1$ as a divisor.
5. Hope that $p - 1$ has only small factors, say 2,3. that only appear a small number of times, say ≤ 3.

Making the Example Work

Want to factor 11227.
If p is a prime factor of 11227. We do not know p.

1. p divides 11227
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm)
3. p divides $2^{k(p-1)} - 1$ mod 11227 for any k
4. Raise 2 to a power that we hope has $p - 1$ as a divisor.
5. Hope that $p - 1$ has only small factors, say 2,3. that only appear a small number of times, say ≤ 3.

$$\mathrm{GCD}(2^{2^3 \times 3^3} - 1 \bmod 11227, 11227) = \mathrm{GCD}(2^{216} - 1 \bmod 11227, 11227)$$

$$= \mathrm{GCD}(1417, 11227) = 109$$

Making the Example Work

Want to factor 11227.
If p is a prime factor of 11227. We do not know p.

1. p divides 11227
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm)
3. p divides $2^{k(p-1)} - 1 \bmod 11227$ for any k
4. Raise 2 to a power that we hope has $p - 1$ as a divisor.
5. Hope that $p - 1$ has only small factors, say 2,3. that only appear a small number of times, say ≤ 3.

$$\mathrm{GCD}(2^{2^3 \times 3^3} - 1 \bmod 11227, 11227) = \mathrm{GCD}(2^{216} - 1 \bmod 11227, 11227)$$

$$= \mathrm{GCD}(1417, 11227) = 109$$

Great! We got a factor of 11227 without having to factor!

Making the Example Work

Want to factor 11227.
If p is a prime factor of 11227. We do not know p.

1. p divides 11227
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm)
3. p divides $2^{k(p-1)} - 1$ mod 11227 for any k
4. Raise 2 to a power that we hope has $p - 1$ as a divisor.
5. Hope that $p - 1$ has only small factors, say 2,3. that only appear a small number of times, say ≤ 3.

$$\mathrm{GCD}(2^{2^3 \times 3^3} - 1 \bmod 11227, 11227) = \mathrm{GCD}(2^{216} - 1 \bmod 11227, 11227)$$

$$= \mathrm{GCD}(1417, 11227) = 109$$

Great! We got a factor of 11227 without having to factor!
Why Worked 109 was a factor and $108 = 2^2 \times 3^3$, small factors.

General Idea

Fermat's Little Theorem if p is prime and a is coprime to p then $a^{p-1} \equiv 1 \pmod{p}$.

General Idea

Fermat's Little Theorem if p is prime and a is coprime to p then $a^{p-1} \equiv 1 \pmod{p}$.

Idea $a^{p-1} - 1 \equiv 0 \pmod{p}$. Pick an a at random. If p is a factor of N then

- p divides $a^{p-1} - 1$ (always)
- p divides N (our hypothesis)
- Hence $\mathrm{GCD}(a^{p-1} - 1 \bmod N, N)$ will be a factor of N.

General Idea

Fermat's Little Theorem if p is prime and a is coprime to p then $a^{p-1} \equiv 1 \pmod{p}$.

Idea $a^{p-1} - 1 \equiv 0 \pmod{p}$. Pick an a at random. If p is a factor of N then

- p divides $a^{p-1} - 1$ (always)
- p divides N (our hypothesis)
- Hence $\mathrm{GCD}(a^{p-1} - 1 \bmod N, N)$ will be a factor of N.

Two problems

- The GCD might be 1 or N. Thats okay- we can try another a.
- We don't have p. If we did, we'd be done!

Do You Believe in Hope?

$a^{p-1} \equiv 1 \pmod{p}$. So for all k, $a^{k(p-1)} \equiv 1 \pmod{p}$.
Idea Let M be a number with LOTS of factors. Hope that $p-1$ is one of them. Pick a at random

$$\mathrm{GCD}(a^M - 1, N) \text{ is non-trivial factor of } N \text{ if Hope is correct.}$$

Do You Believe in Hope?

$a^{p-1} \equiv 1 \pmod{p}$. So for all k, $a^{k(p-1)} \equiv 1 \pmod{p}$.
Idea Let M be a number with LOTS of factors. Hope that $p-1$ is one of them. Pick a at random

$$\mathrm{GCD}(a^M - 1, N) \text{ is non-trivial factor of } N \text{ if Hope is correct.}$$

How could we not get a non-trivial factor?

- $\mathrm{GCD}(a^M - 1, N) = 1$. So $p-1$ does not divide M. M needs to have more factors in it.
- $\mathrm{GCD}(a^M - 1, N) = N$. So $a^M - 1$ has $p-1$ and $\frac{N}{p-1}$ in it. Need M to have less factors.

Want M to have lots of small factors so avoids prob 1.
Want M to have not so many factors so avoids prob 2.

Do You Believe in Hope?

Hope Want pick M with many small factors, but might adjust. Let B be a parameter. Will let

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

- If B is big then gets lots of factors.
- If B is small then do not get that many factors.
- Goldilocks Problem–want B that is just right.
- Can't quite do that. Instead we try a B and then adjust it.

Example of B, M

Let B be a parameter.

$$M = \prod_{q \leq B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$
$q = 2$, $\lceil \log_2(10) \rceil = 4$. So 2^4.

Example of B, M

Let B be a parameter.

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$
$q = 2$, $\lceil \log_2(10) \rceil = 4$. So 2^4.
$q = 3$, $\lceil \log_3(10) \rceil = 4$. So 3^4.

Example of B, M

Let B be a parameter.

$$M = \prod_{q \leq B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$
$q = 2$, $\lceil \log_2(10) \rceil = 4$. So 2^4.
$q = 3$, $\lceil \log_3(10) \rceil = 4$. So 3^4.
$q = 5$, $\lceil \log_5(10) \rceil = 2$. So 5^2.

Example of B, M

Let B be a parameter.

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$

$q = 2$, $\lceil \log_2(10) \rceil = 4$. So 2^4.
$q = 3$, $\lceil \log_3(10) \rceil = 4$. So 3^4.
$q = 5$, $\lceil \log_5(10) \rceil = 2$. So 5^2.
$q = 7$, $\lceil \log_7(10) \rceil = 2$. So 7^2.

Example of B, M

Let B be a parameter.

$$M = \prod_{q \leq B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$
$q = 2$, $\lceil \log_2(10) \rceil = 4$. So 2^4.
$q = 3$, $\lceil \log_3(10) \rceil = 4$. So 3^4.
$q = 5$, $\lceil \log_5(10) \rceil = 2$. So 5^2.
$q = 7$, $\lceil \log_7(10) \rceil = 2$. So 7^2.

$$M = 2^4 \times 3^4 \times 5^2 \times 7^2$$

If $p - 1$ only has factors $2, 3, 5, 7$, and if 2 appears ≤ 4 times, 3 appears ≤ 4 times, 5 appears ≤ 2 times, 7 appears ≤ 2 times then

$$\mathrm{GCD}(a^M - 1, N) \text{ Will be a multiple of } p.$$

Do You Believe in Hope? The Algorithm

Parameter B and hence also

$$M = \prod_{q \leq B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

```
FOUND = FALSE
while NOT FOUND
     a=RAND(1,N-1)
     d=GCD(a^M-1,N)
     if d=1 then increase B
     if d=N then decrease B
     if (d NE 1,N) then FOUND=TRUE
output(d)
```

Do You Believe in Hope? The Algorithm

Parameter B and hence also

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

```
FOUND = FALSE
while NOT FOUND
     a=RAND(1,N-1)
     d=GCD(a^M-1,N)
     if d=1 then increase B
     if d=N then decrease B
     if (d NE 1,N) then FOUND=TRUE
output(d)
```

FACT If $p-1$ has all factors $\le B$ then runtime is $B \log B (\log N)^2$.

Do You Believe in Hope? The Algorithm

Parameter B and hence also

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

```
FOUND = FALSE
while NOT FOUND
     a=RAND(1,N-1)
     d=GCD(a^M-1,N)
     if d=1 then increase B
     if d=N then decrease B
     if (d NE 1,N) then FOUND=TRUE
output(d)
```

FACT If $p-1$ has all factors $\le B$ then runtime is $B \log B (\log N)^2$.
FACT B big then runtime Bad but prob works.

Do You Believe in Hope? The Algorithm

Parameter B and hence also

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

```
FOUND = FALSE
while NOT FOUND
      a=RAND(1,N-1)
      d=GCD(a^M-1,N)
      if d=1 then increase B
      if d=N then decrease B
      if (d NE 1,N) then FOUND=TRUE
output(d)
```

FACT If $p-1$ has all factors $\le B$ then runtime is $B \log B (\log N)^2$.
FACT B big then runtime Bad but prob works.
FACT Works well if $p-1$ only has small factors.

In Practice

A rule-of-thumb in practice is to take $B \sim N^{1/6}$.

1. Fairly big so the M will be big enough.
2. Run time $N^{1/6}(\log N)^3$ pretty good, though still exp in $\log N$.
3. Warning This does not mean we have an $N^{1/6}(\log N)^3$ algorithm for factoring. It only means we have that if $p-1$ has all factors $\leq N^{1/6}$.

Advice for Zelda When she uses RSA

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

1. When pick $N_i = p_i q_i$, make sure $p_i - 1$ and $q_i - 1$ have some large factors.
2. Either e_i's different or if all are e, then e large.
3. If all the e's are the same, pad m so m^e large.
4. Either N_i different or if all are N, e_i's not rel prime.
5. Randomly pad m for NY,NY problem.
6. Randomly pad time to ward of timing attacks.