BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

The Same N Attack on RSA

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

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

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!

Review of RSA Attacks

1. If same e, $e \leq L$. 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!
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:

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

How about

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

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?

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, 408 are relatively prime. Lets find combo that adds to 1.

341 and 408 are Rel Prime

341, 408 are relatively prime. Lets find combo that adds to 1.

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

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 $m^{408} \pmod{1147}$.

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 $m^{408} \pmod{1147}$.

Eve does the following:

- Finds 1 as a combo of 341 and 408: $1 = 56 \times 408 - 67 \times 341$
- 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 $m^{408} \pmod{1147}$.

Eve does the following:

- Finds 1 as a combo of 341 and 408: $1 = 56 \times 408 - 67 \times 341$
- Find inverse of m^{341} mod 1147. We call this m^{-341}.
- Compute mod 1147:

$$(m^{408})^{56} \times (m^{-341})^{67} \equiv m^{56\times408-67\times341} \equiv m^1 \equiv m$$

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 $m^{408} \pmod{1147}$.

Eve does the following:

- Finds 1 as a combo of 341 and 408: $1 = 56 \times 408 - 67 \times 341$
- 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 Alice, Bob, and Carol. Eve sees

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

Example Continued

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

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

Eve does the following:

- Finds 1 as combo of ...: $27 \times 35 - 17 \times 100 + 6 \times 126 = 1$
- Find inverse of m^{100} mod 1147. We call this m^{-100}.

Example Continued

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

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

Eve does the following:

- Finds 1 as combo of ...: $27 \times 35 - 17 \times 100 + 6 \times 126 = 1$
- Find inverse of m^{100} mod 1147. We call this m^{-100}.
- Compute mod 1147:

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

Example Continued

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

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

Eve does the following:

- Finds 1 as combo of ...: $27 \times 35 - 17 \times 100 + 6 \times 126 = 1$
- Find inverse of m^{100} mod 1147. We call this m^{-100}.
- Compute mod 1147:

$$(m^{35})^{27} \times (m^{-100})^{17} \times (m^{126})^{6} \equiv m^{27\times35-17\times100+6\times126} \equiv m^1 \equiv m$$

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!).

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 and Bob. 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 and Bob. Eve sees

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

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

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 and Bob. Eve sees

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

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

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

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 and Bob. 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 and Bob. 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 $\exists\ x_1, \ldots, x_L \in \mathbb{Z}$, $\sum_{i=1}^{L} e_i x_i = 1$.

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} (mod N).
$e_1, \ldots, e_L$ rel prime, so $\exists\ x_1, \ldots, x_L \in \mathbb{Z}$, $\sum_{i=1}^{L} e_i x_i = 1$. Eve finds $x_1, \ldots, x_L$ and then computes

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

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 $\exists\ x_1, \ldots, x_L \in \mathbb{Z}$, $\sum_{i=1}^{L} e_i x_i = 1$. Eve finds $x_1, \ldots, x_L$ and then computes

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

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} (mod N).
$e_1, \ldots, e_L$ rel prime, so $\exists\ x_1, \ldots, x_L \in \mathbb{Z}$, $\sum_{i=1}^{L} e_i x_i = 1$. Eve finds $x_1, \ldots, x_L$ and then computes

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

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 $\exists\ x_1, \ldots, x_L \in \mathbb{Z}$, $\sum_{i=1}^{L} e_i x_i = 1$. Eve finds $x_1, \ldots, x_L$ and then computes

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

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, $ax_1 + bx_2 = 1$.

Generalization ONE Let $d = \mathrm{GCD}(a, b)$.

Then exists x_1, x_2 such that $ax_1 + bx_2 = d$.

Good News Euclidean Alg finds d, x_1, x_2.

An Example

Recall If a, b rel prime then exists x_1, x_2, $ax_1 + bx_2 = 1$.
Generalization ONE Let $d = \mathrm{GCD}(a, b)$.

Then exists x_1, x_2 such that $ax_1 + bx_2 = d$.

Good News Euclidean Alg finds d, x_1, x_2.

What About $\mathrm{GCD}(a, b, c)$?

An Example

Recall If a, b rel prime then exists x_1, x_2, $ax_1 + bx_2 = 1$.
Generalization ONE Let $d = \mathrm{GCD}(a, b)$.

Then exists x_1, x_2 such that $ax_1 + bx_2 = d$.

Good News Euclidean Alg finds d, x_1, x_2.

What About $\mathrm{GCD}(a, b, c)$?

Generalization TWO Let $d = \mathrm{GCD}(a, b, c)$.
Then exists x_1, x_2, x_3 such that $ax_1 + bx_2 + cx_3 = d$.

An Example

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

Generalization ONE Let $d = \mathrm{GCD}(a, b)$.

Then exists x_1, x_2 such that $ax_1 + bx_2 = d$.

Good News Euclidean Alg finds d, x_1, x_2.

What About $\mathrm{GCD}(a, b, c)$?

Generalization TWO Let $d = \mathrm{GCD}(a, b, c)$.

Then exists x_1, x_2, x_3 such that $ax_1 + bx_2 + cx_3 = d$.

Example We find a combination of 35, 100, 126 that sums to 1.

Want $x, y, z \in \mathbb{Z}$ Such That $35x + 100y + 126z = 1$

Want $x, y, z \in \mathbb{Z}$ Such That $35x + 100y + 126z = 1$

1. Find x_1, x_2 such that $35x_1 + 100x_2 = \mathbf{5}$ (5=GCD(35,100))

$$35 \times 3 - 100 = \mathbf{5}$$

Want $x, y, z \in \mathbb{Z}$ Such That $35x + 100y + 126z = 1$

1. Find x_1, x_2 such that $35x_1 + 100x_2 = \mathbf{5}$ (5=GCD(35,100))

$$35 \times 3 - 100 = \mathbf{5}$$

2. Find y_1, y_2 such that $\mathbf{5}y_1 + 126y_2 = 1$

$$-25 \times \mathbf{5} + 126 = 1$$

Want $x, y, z \in \mathbb{Z}$ Such That $35x + 100y + 126z = 1$

1. Find x_1, x_2 such that $35x_1 + 100x_2 = \mathbf{5}$ (5=GCD(35,100))

$$35 \times 3 - 100 = \mathbf{5}$$

2. Find y_1, y_2 such that $\mathbf{5}y_1 + 126y_2 = 1$

$$-25 \times \mathbf{5} + 126 = 1$$

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

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

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

Algorithm for x_1, x_2, x_3

This will be on a HW

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 $(N_i = p_i q_i, e_i)$

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. Make all of the e_i's different

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. Make all of the e_i's different
2. Make all of the N_i's different.

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. Make all of the e_i's different
2. Make all of the N_i's different.
3. Randomly pad m for NY,NY problem.

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. Make all of the e_i's different
2. Make all of the N_i's different.
3. Randomly pad m for NY,NY problem.
4. Randomly pad time to ward off timing attacks.

BILL, STOP RECORDING LECTURE!!!!

BILL STOP RECORDING LECTURE!!!