DTTF/NB479: Dszquphsbqiz Day 10

- Announcements:
  - Computer exam **next class**
- Questions?

Tomorrow's exam

For each problem, I'll specify the algorithm:

Shift   Affine   Vigenere   Hill

and the attack:

Ciphertext only   known plaintext

- You may use code that you wrote or that you got from the textbook.
- May require you to modify your code some on the fly
- Have your algorithms ready to run…

Can we generalize Fermat's little theorem to composite moduli?

The three-pass protocol is an application of Fermat's little theorem to key exchange

- How can Alice get a secret message to Bob without an established key?

- Can do it with locks.
- First 2 volunteers get to do a live demo

The three-pass protocol is an application of Fermat's little theorem to key exchange

- Situation: Alice wants to get a short message to Bob, but they don't have an established key to transmit it.
- Can do with locks:

The three-pass protocol is an application of Fermat's little theorem to key exchange

- Situation: Alice wants to get a short message to Bob, but they don't have an established key to transmit it.
- Can do with locks:

The three-pass protocol is an application of Fermat's little theorem to key exchange

- Situation: Alice wants to get a short message to Bob, but they don't have an established key to transmit it.
- Can do with locks:



The three-pass protocol is an application of Fermat's little theorem to key exchange

- Situation: Alice wants to get a short message to Bob, but they don't have an established key to transmit it.
- Can do with locks:

Note: it's always secured by one of their locks

In the three-pass protocol, the "locks" are random numbers that satisfy specific properties

- K: the secret message
- p: a large public prime number > K
- The two locks:
  - a: Alice's random #, gcd(a,p-1)=1
  - b: Bob's random #, gcd(b,p-1)=1
- To unlock their locks:
  - a^{-1} mod (p-1)
  - b^{-1} mod (p-1)

In the three-pass protocol, the “locks” are random numbers that satisfy specific properties

- K: the secret message
- p: a public prime number > K
- The two locks:
  - a: Alice’s random #, gcd(a,p-1)=1
  - b: Bob’s random #, gcd(b,p-1)=1
- To unlock their locks:
  - a^{-1} mod (p-1)
  - b^{-1} mod (p-1)

Three-pass protocol:

Alice computes K^a (mod p) and sends to Bob

Bob computes $(K^a)^b$ (mod p) and sends it back

Alice computes $((K^a)^b)^{a^{-1}}$ (mod p) and sends it back

Bob computes $(((K^a)^b)^{a^{-1}})^{b^{-1}}$ (mod p) and reads K

In the three-pass protocol, the "locks" are random numbers that satisfy specific properties

- 36 K: the secret message
- 59 p: a public prime number > K
- The two locks:
  - 17 a: Alice's random #, gcd(a,p-1)=1
  - 21 b: Bob's random #, gcd(b,p-1)=1
- To unlock their locks:
  - 41 a^{-1} mod (p-1)
  - 47 b^{-1} mod (p-1)

Three-pass protocol:

Alice computes K^a (mod p) and sends to Bob

Bob computes $(K^a)^b$ (mod p) and sends it back

Alice computes $((K^a)^b)^{a^{-1}}$ (mod p) and sends it back

Bob computes $(((K^a)^b)^{a^{-1}})^{b^{-1}}$ (mod p) and reads K

Toy example:

36^{17} (mod 59) = 12

12^{21} (mod 59) = 45

45^{41} (mod 59) = 48

48^{47} (mod 59) = 36

Why does it work?

The basic principle relates the moduli of the expressions to the moduli in the exponents

- When dealing with numbers mod n, we can deal with their exponents mod ______

- So…
  - Given integers a and b,
  - Since $aa^{-1}=bb^{-1}=1 \pmod{p-1}$
  - …what's $K^{(aba^{-1}b^{-1})} \pmod{p}$?

Why isn’t this used in key exchange today?

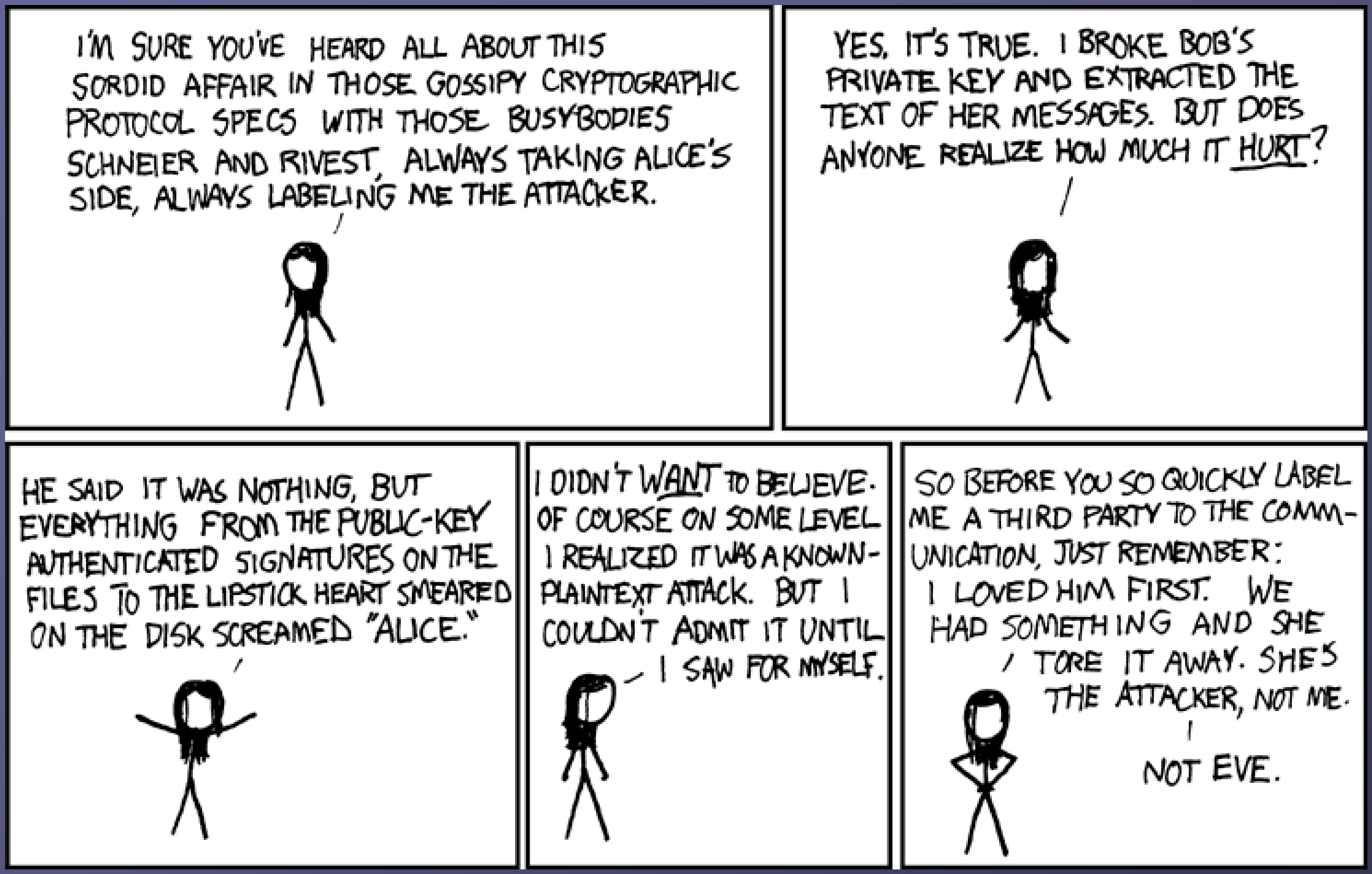
- Trappe and Washington say that it’s vulnerable to an “intruder-in-the-middle” attack. Think about this…

You are now prepared to read as much of the rest of chapter 3 as you like

- We’ll revisit 3.7 (primitive roots) and 3.11 (fields) later
- The rest is more number theory fun.

- Tomorrow we start DES

Maybe Alice and Bob's exchange wasn't as secure as they thought…



http://xkcd.com/c177.html

Yet one more reason I'm barred from speaking at crypto conferences.