Cryptography for Dummies – 2
From Classical to Modern

Laszlo Csirmaz

Central European University

March 26–30, 2012

Cryptographic Attacks

Protect the system, not the components!

Protect the right thing.

Cryptographic Attacks

Protect the system, not the components!

- Don't put a bank vault door on a tent.

Protect the right thing.

Cryptographic Attacks

Protect the system, not the components!

- Don't put a bank vault door on a tent.
- The chain is as strong as its weakest link.

Protect the right thing.

Cryptographic Attacks

Protect the system, not the components!

- Don't put a bank vault door on a tent.
- The chain is as strong as its weakest link.

Protect the right thing.

- Utility meters protect the amount of money actually put into them,

Cryptographic Attacks

Protect the system, not the components!

- Don't put a bank vault door on a tent.
- The chain is as strong as its weakest link.

Protect the right thing.

- Utility meters protect the amount of money actually put into them, **but not the unit price!**

Cryptographic Attacks

Protect the system, not the components!

- Don't put a bank vault door on a tent.
- The chain is as strong as its weakest link.

Protect the right thing.

- Utility meters protect the amount of money actually put into them, **but not the unit price!**
- Bank cards protect the PIN code,

Cryptographic Attacks

Protect the system, not the components!

- Don't put a bank vault door on a tent.
- The chain is as strong as its weakest link.

Protect the right thing.

- Utility meters protect the amount of money actually put into them, **but not the unit price!**
- Bank cards protect the PIN code,
  but not the account number!

Attacks on primitives

Not to be overlooked:

new designs have new mistakes!

Known plaintext attack

The adversary can acquire both the unscrambled **and** the scrambled version of the same message.

Examples:

1. Capturing the same message both in plain and encrypted (after a complain that the message did not arrive)
2. WiFi beam packages are broadcasted clear, and then encrypted
3. WinZip has know values encrypted at places: use `pkcrack`

Attacks on primitives

Chosen plaintext attack

The adversary can enforce encrypting a message of his choice

1. British secret service advertising in Turkish newspapers.
2. WWII: Japan diplomat asked as a "favor" to send a message using the most secret diplomatic code.
3. use a cryptocard (or public service) to electronically sign messages of my choice

Attacks on primitives

Chosen ciphertext attack

The adversary chooses the scrambled message which will be unscrambled (and acted upon) by the honest party

1. Capture some message, alter it in certain places and send it back (IP spoofing of encrypted packages – can be done using WiFi)
2. the *one million chosen ciphertext attack* on https protocol
3. attacks on RSA encryption and signing
   Alice signs any message with her public key

Attacks on primitives

Birthday attack

The chances that two out of 23 people have the same birthday is greater than 50 percent.
Only a relatively small number of trials are necessary to get two identical outcomes. To get two texts with the same 6 digit digest (hash value), you need to try only 1000 random texts.

Man in the Middle attack

It is easy to beat on of *two chess masters* at the same time: you need to pass the steps of one to the other.

1. Bob sends his public key to Alice, but Eve captures the message and pretends to be Alice. Bob won't notice the difference, thus talks to Eve confidentially.
2. *identity hijacking*

Attacks on primitives

Side channel attack

You do what no one was expecting:

1. put your credit card into the microwave
2. measure the current consumption of the chip card
3. put chipcards to the fridge
4. listen the "sound of encrypting" of the processor

Social engineering

"Important message!
This is an important security notice. To prevent password stealing, you must re-register. Please visit our web page, or reply to this e-mail by providing your full name, telephone, login name, password."

Attacks on primitives

And, last, but not least:

Attacks on primitives

And, last, but not least:

Rubber Hose attack

Beat your enemy until he gives up the secret!