A HANDS-ON INTRO TO INTERNET SECURITY

Mike Hughes

5 March 2010

Today's Roadmap

1) Motivation: Internet Security for Everyone

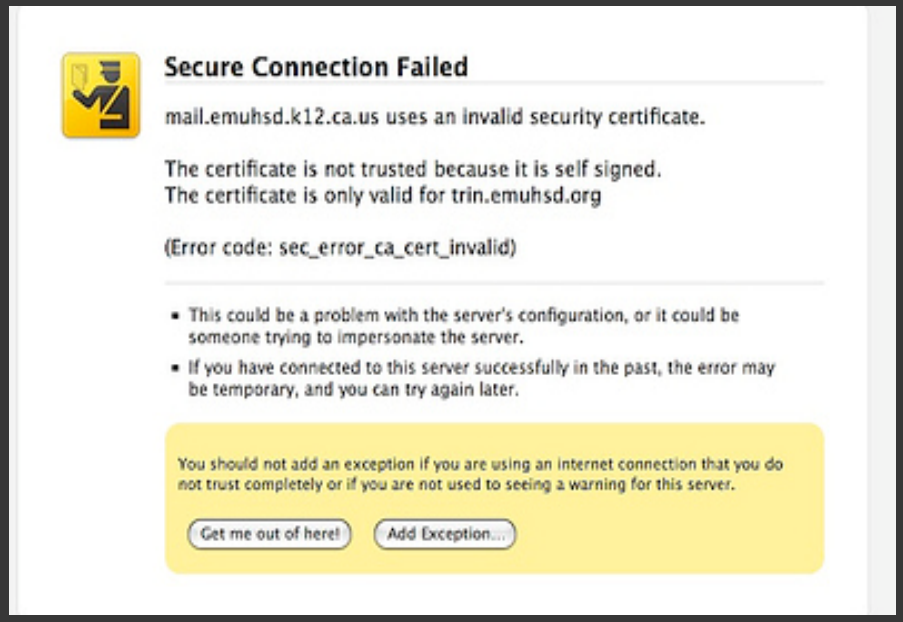
2) Puzzle: Situated Active Learning for Novices

3) Proposal: Hands-on Design Challenges

4) Results: Victories and Revisions

Motivation

Internet users of all stripes encounter screens like this every day…



But what makes a website trustworthy?

Isn't this something everyone should understand?

Lesson Goals

- Understand **privacy** and **authentication**
  - The Why: risks, consequences
  - The How: technology, protocols
  - The Challenges: assumptions, limitations

today's focus

- Connect to **everyday browsing**

Competencies:

lifelong learning

qualitative analysis

Puzzle

How can I explain complicated ideas like trusted third parties and digital certificates to complete beginners ?

Disciplinary Barriers

- inaccessible tech

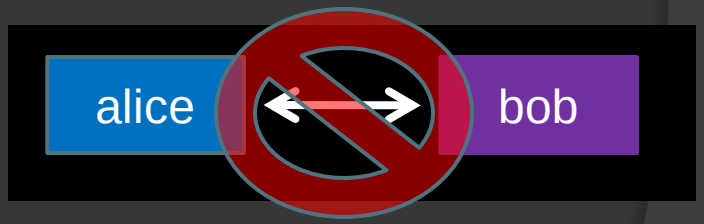
$$m^e \equiv c \pmod{n}.$$

- jargon

"public key"
"cipher text"
"CA"

Pedagogical Barriers

- authentic problems



- active learning

motivation, confidence
important for novices
especially in CS

Proposal: Series of Design Challenges

Inquiry-based, team competitions

using hands-on crypto software designed for novices.

Situated in authentic context

Online banking

Roles: Bank, Customer, Attacker

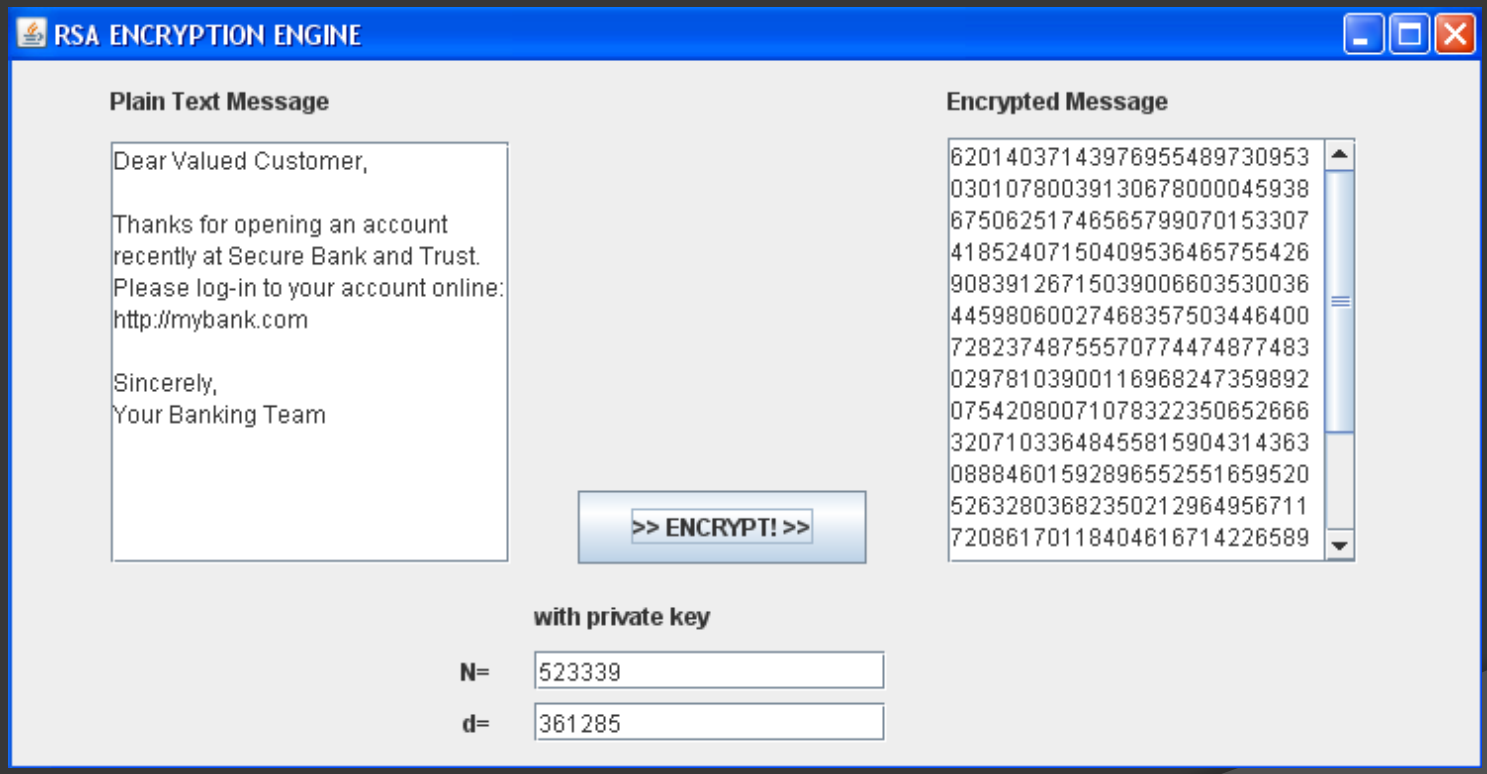
Progressively build domain knowledge

1) encryption basics
2) key vulnerability
3) third-party key exchange
4) digital certificate
5) certificate authority

Hands-on Crypto for Novices

Allows **authentic** messages

supports **experimentation**



Few parameters, **simple** graphic interface

Example Design Challenge

Develop an encryption protocol that an intruder with full access to the transmitted message could not break after 1 minute

1

Arrange teams

Bank

Customer

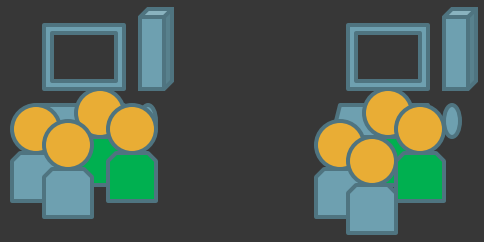
Example Design Challenge

Develop an encryption protocol that an intruder with full access to the transmitted message could not break after 1 minute

2

Plan for 5 minutes

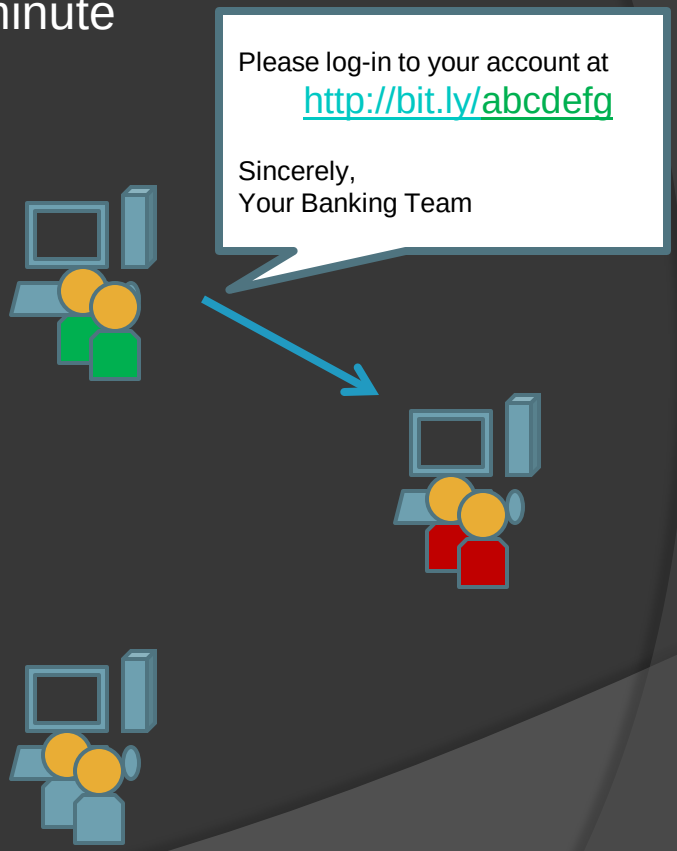
Bank



Customer

Example Design Challenge

Develop an encryption protocol that an intruder with full access to the transmitted message could not break after 1 minute



3

Bank sends Encrypted Message to Attacker

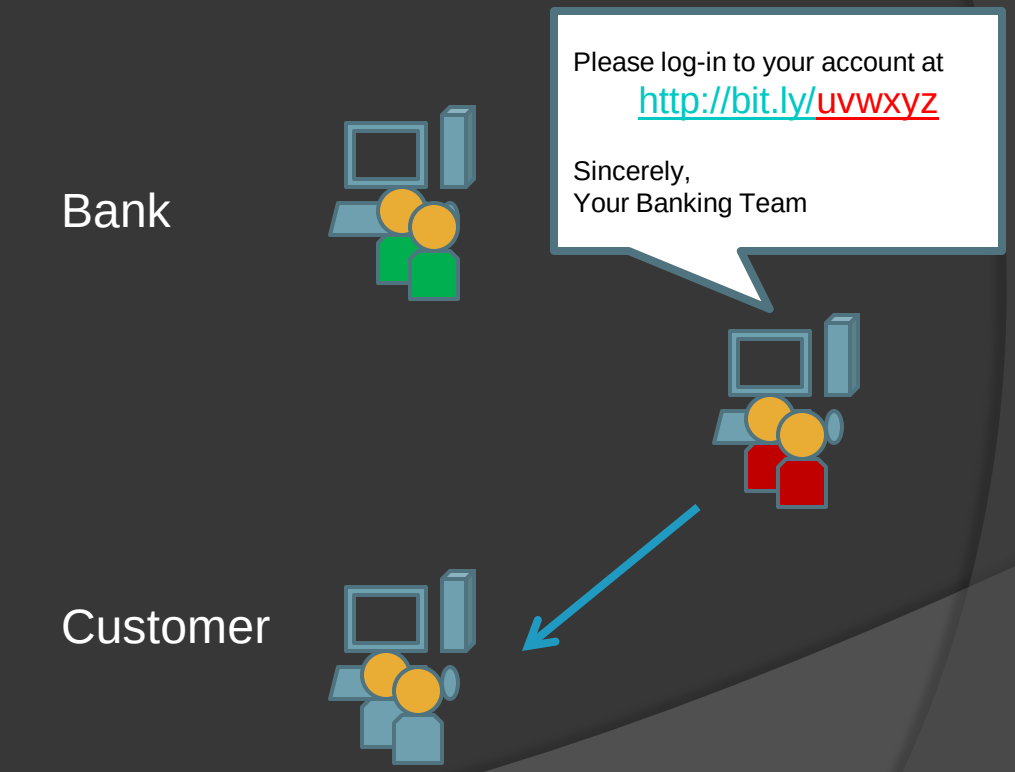
Example Design Challenge

Develop an encryption protocol that an intruder with full access to the transmitted message could not break after 1 minute

4

Attacker tries to hack message for 1 minute

Then relays either message to customer

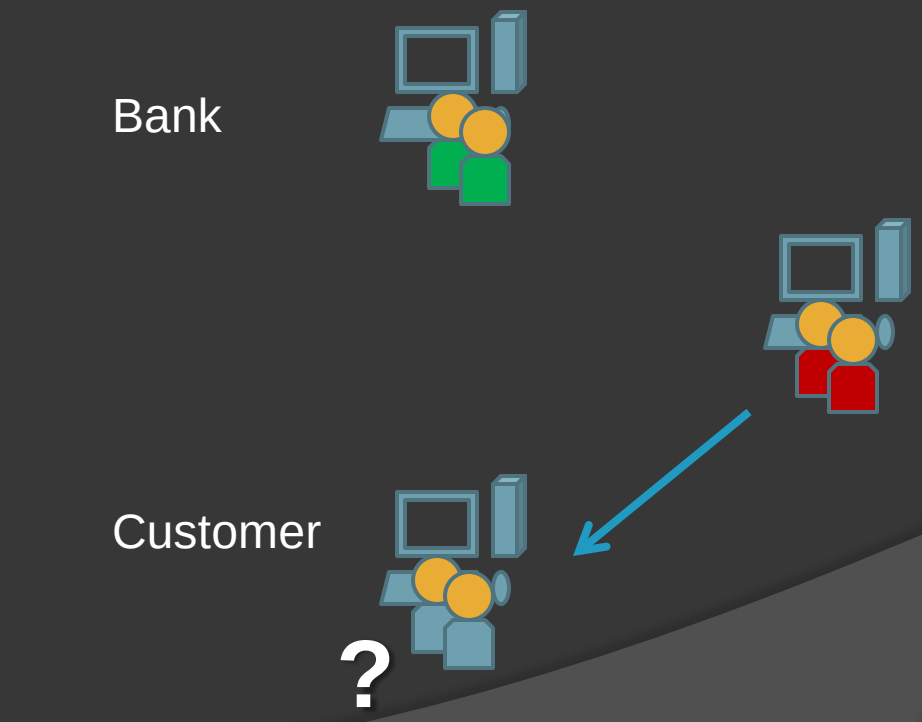


Example Design Challenge

Develop an encryption protocol that an intruder with full access to the transmitted message could not break after 1 minute

5

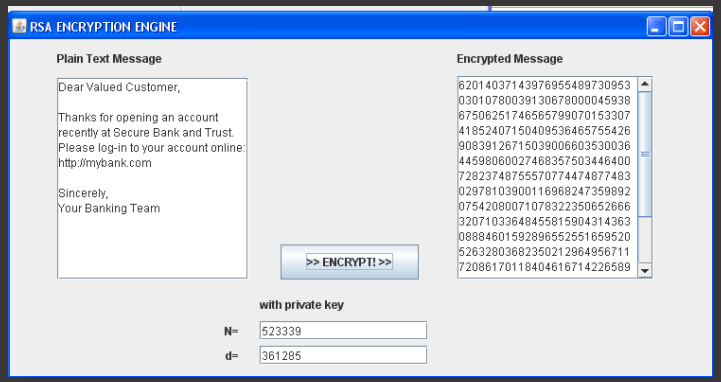
Customer decrypts message, decides "Do I trust this link?"



Design Challenge Advantages

Disciplinary

- accessible tech



- jargon

slowly built as needed by student progress

Pedagogical

- authentic problems

online banking

- active learning

open-ended hands-on teams

Results

Taught 6 students for 90 minutes

Made it through 4.5 design challenges.

They said:

“exciting” *“fun”* *“not bored”*

Victories

Students discovered their own knowledge!

Encryption as a composable function

encrypt(encrypt(msg))

Larger keys are exponentially more difficult to break

Random padding and substitution

… while having fun!

"I bet you can't hack this now… try it!".

Struggles

- Balancing instructor attention
- Giving clear instructions
- Recap knowledge after each challenge

Remaining Questions

- Scalability
  - Does it work in large classrooms?
- Share-ability
  - Can others use this out-of-the-box?

Does it really take this long to develop good active learning curriculum?