

A HANDS-ON INTRO TO INTERNET SECURITY

Mike Hughes

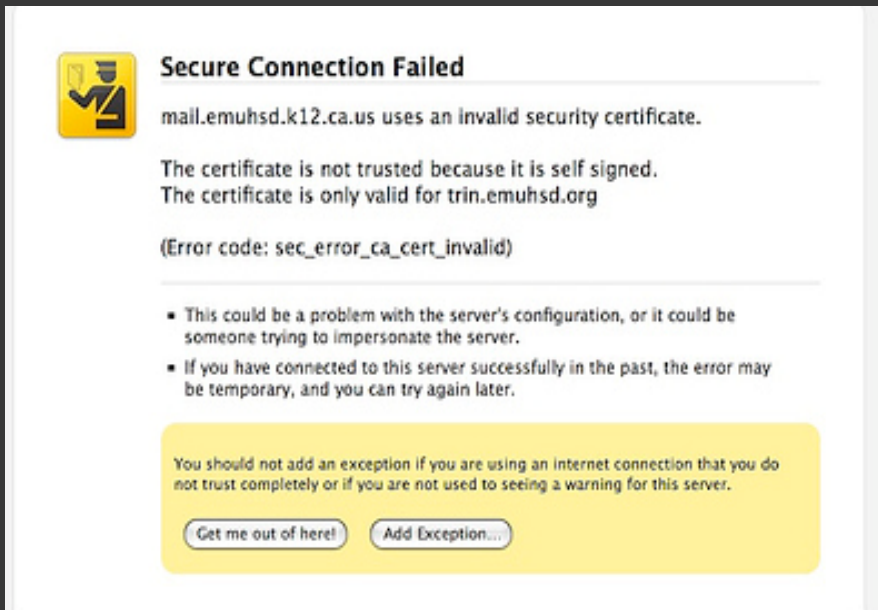
5 March 2010

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...



Secure Connection Failed

mail.emuhd.k12.ca.us uses an invalid security certificate.

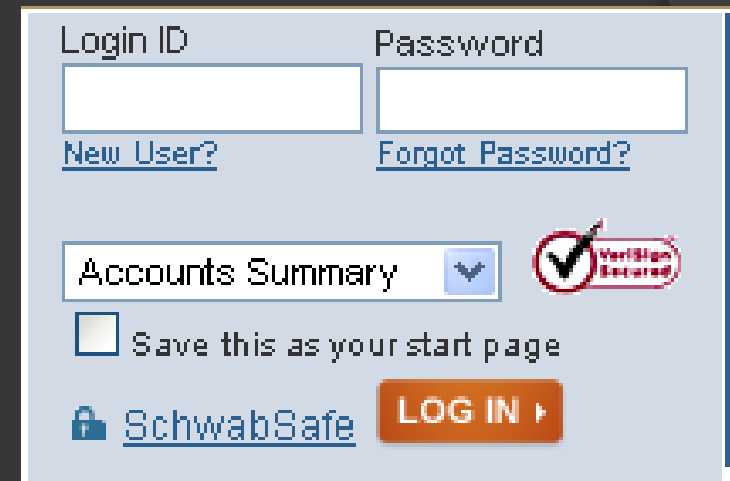
The certificate is not trusted because it is self signed.
The certificate is only valid for trin.emuhd.org

(Error code: sec_error_ca_cert_invalid)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.


You should not add an exception if you are using an Internet connection that you do not trust completely or if you are not used to seeing a warning for this server.

[Get me out of here!](#) [Add Exception...](#)



Login ID Password

[New User?](#) [Forgot Password?](#)

Accounts Summary 

Save this as your start page

[SchwabSafe](#)

But what makes a website **trustworthy**?

Isn't this something **everyone** should understand?

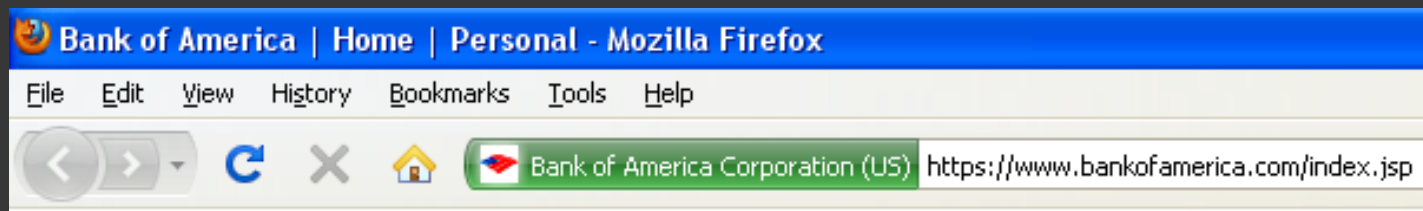
Lesson Goals

◎ 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

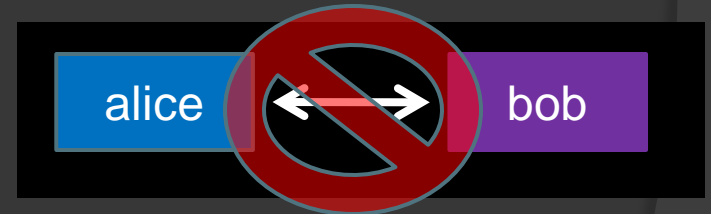
$$m^e \equiv c \pmod{n}.$$

- 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**

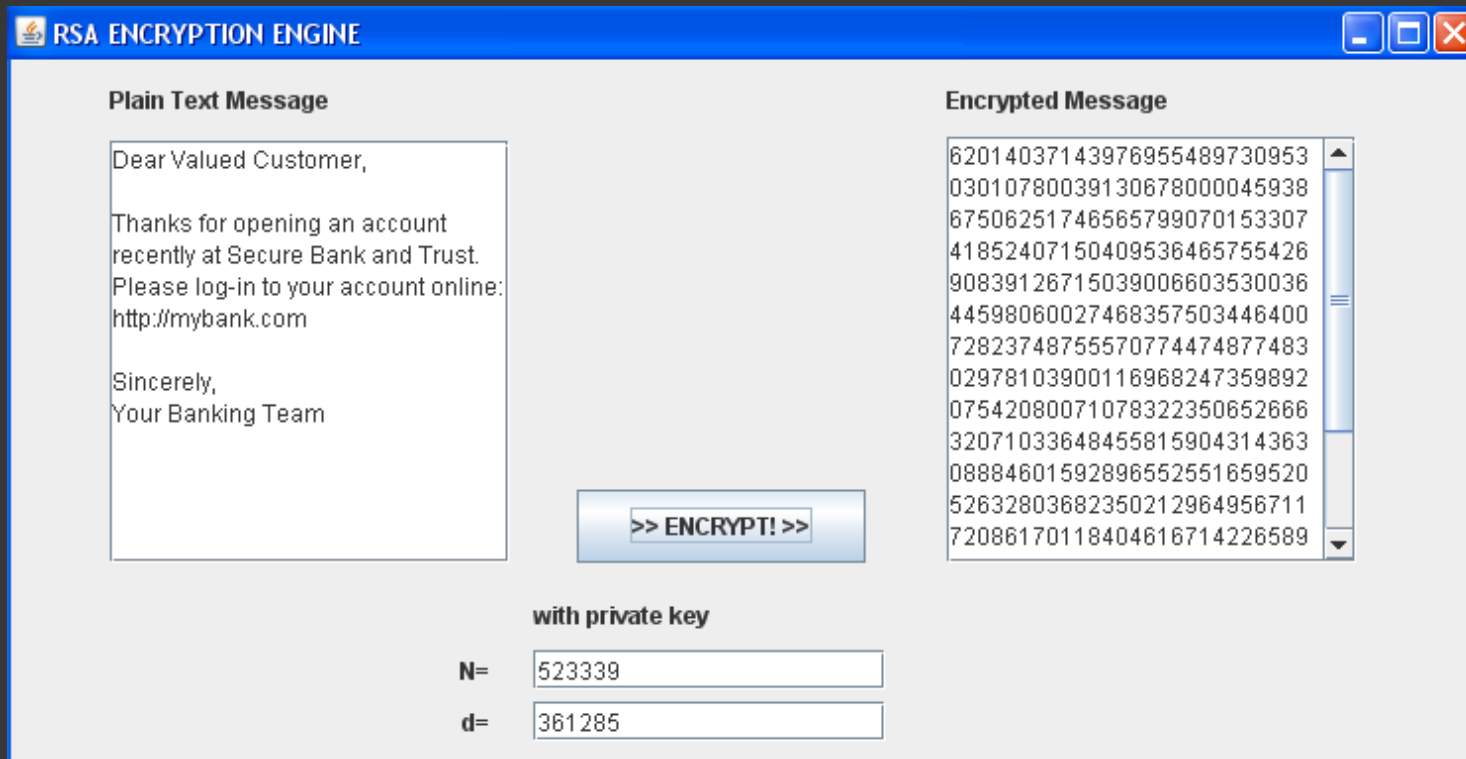
Progressively build domain knowledge

- 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**



The screenshot shows a window titled "RSA ENCRYPTION ENGINE". It is divided into two main sections: "Plain Text Message" and "Encrypted Message".

Plain Text Message:

Dear Valued Customer,

Thanks for opening an account recently at Secure Bank and Trust. Please log-in to your account online: <http://mybank.com>

Sincerely,
Your Banking Team

Encrypted Message:

```
62014037143976955489730953
03010780039130678000045938
67506251746565799070153307
41852407150409536465755426
90839126715039006603530036
44598060027468357503446400
72823748755570774474877483
02978103900116968247359892
07542080071078322350652666
32071033648455815904314363
08884601592896552551659520
52632803682350212964956711
72086170118404616714226589
```

>> ENCRYPT! >>

with private key

N=

d=

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

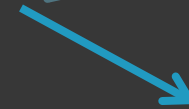
3

*Bank sends
Encrypted Message
to Attacker*

Bank



Please log-in to your account at
<http://bit.ly/abcdefg>
Sincerely,
Your Banking Team



Customer



Example Design Challenge

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

4

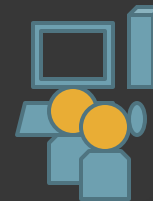
Attacker tries to hack message for 1 minute

Then relays either message to customer

Bank



Customer



Please log-in to your account at
<http://bit.ly/uvwxyz>
Sincerely,
Your Banking Team



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?"

Bank



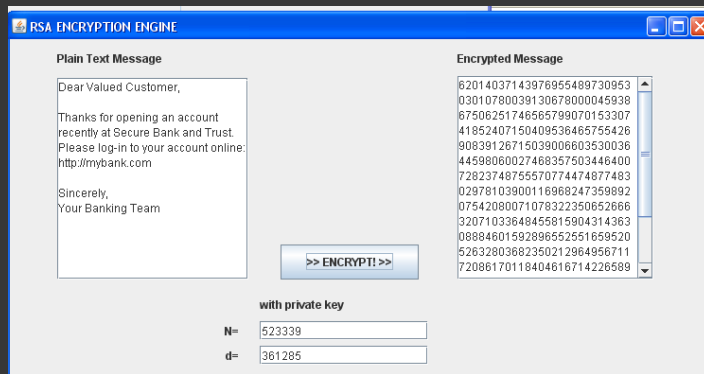
Customer



Design Challenge Advantages

Disciplinary

- accessible tech



Pedagogical

- authentic problems

online banking

- jargon

*slowly built as needed
by student progress*

- 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?