Cryptography: Basics & Applications

2013 JMU Cyber Defense Boot Camp

What is this unit about?

- Lecturing
  - "**Boring**" lecturing (practice in next session)
- A topic that has challenged the human kind for more than 2000 years
  - Dated beyond Julius Caesar (around 56 BC)

- Slides are available at https://users.cs.jmu.edu/tjadenbc/Bootcamp/3-crypto.pdf

Organization

- The data confidentiality problem
- Theory
  - Numbers
  - Encryption
  - Digital signature
  - Cryptographic hashing
  - Digital certificates and PKI
- Tie everything together: HTTPS

Focus on concepts;

Skip details

Road Map

- The data confidentiality problem
- Theory
  - Numbers
  - Encryption
  - Digital signature
  - Cryptographic hashing
  - Digital certificates and PKI
- Tie everything together: HTTPS

Questions

- How do you protect (the **confidentiality** of) your Turbo Tax file on your computer?
  - Full name, SSN, DOB, home address

- How do you protect the financial information on your computer?
  - Bank accounts, retirement plan accounts, stock investment accounts

Encrypt them?

What is encryption?

What the heck is Cryptography?

- We have heard “encryption” more
- Cryptography
  - Kryptos: hidden
  - -graphy
    - writing or representation in a (specified) manner or by a (specified) means or of a (specified) object
- Traditionally, cryptography = encryption

Welcome to the Wonderful Land

- **Q:** How many cryptographers does it take to change a light bulb?
- **A:** XIGHCBS

Road Map

- The data confidentiality problem
- Theory
  - Numbers
  - Encryption
  - Digital signature
  - Cryptographic hashing
  - Digital certificates and PKI
- Tie everything together: HTTPS

Road Map

- The data confidentiality problem
- Theory
  - Numbers
  - Encryption
  - Digital signature
  - Cryptographic hashing
  - Digital certificates and PKI
- Tie everything together: HTTPS

Warm-up Questions

- $2^3 =$ **?**
- $2^4 =$ **?**
- $2^3 < 10 < 2^4$ **?**

- $\log_2 8 =$ **?**
- $\log_2 16 =$ **?**
- $\log_2 10 =$ **?**

- $\log_2(10^6) =$ **?**
- $\log_2(10^9) =$ **?**

Back-of-Envelope Calculations

- How many seconds are there in a day?

  $24 \times 60 \times 60 = 86{,}400$ seconds

  In 2^{x}?

  $\leq 2^{17}$

How?

$86400 = 2^{x}$

$8 \times 10^{4} \approx 2^{x}$

$$\log_2(8 \times 10^4) \approx \log_2(2^x)$$

$$\log_2 8 + \log_2(10^4) \approx x$$

$$3 + 4 \times \log_2(10) \approx x$$

$$x \approx 16.3$$

Back-of-Envelope Calculations

- How many seconds are there in a day?

  $24 \times 60 \times 60 = 86{,}400$ seconds

  In 2^x?

  $\leq 2^{17}$

$100 \text{ years} \approx 2^{32} \text{ seconds}$

- How many seconds are there **in a year**?

  $365 \text{ days} \times 86{,}400 = 31{,}536{,}000$

  $\leq 2^{25}$

- How many seconds in 100 years?

  $3{,}153{,}600{,}000 \text{ seconds} = 3.1536 \times \mathbf{10^9}$

  $\approx 3.1536 \times 2^{30} \leq \mathbf{2^{32}}$

Seconds in $2^?$

- 1 hour: $60 \times 60 = 3600$ seconds ($\leq 2^{12}$)
- 1 day: $24 \times 60 \times 60 = 86{,}400$ seconds ($\leq 2^{17}$)
- 1 month: $30 \text{ days} \times 86{,}400 = 2592000$ seconds ($< 2^{22}$)
- 1 year: $365 \text{ days} \times 86{,}400 = 31{,}536{,}000$ ($< 2^{25}$)
- 100 years: $3{,}153{,}600{,}000$ seconds $= 3.1536 \times 10^9 \approx 3.1536 \times 2^{30} \leq 2^{32}$

Back-of-Envelope Calculations

- How many “operations” can a computer do in one second?

Intel CPU

- Intel CPU: 3.45GHz
- 3.45×10^9Hz
- Clock rate: 3.45×10^9 times per second
- Assumption: 3.45×10^9 basic operations per second
  - ❖ $3.45\times10^9 < \mathbf{2^{32}}$;
- So in 100 years, this CPU can exhaust $2^{32} \times \mathbf{2^{32}} = 2^{64}$ basic operations

Nov. 14, 2012

- Fastest computer:
  - http://www.top500.org/
- DOE/SC/Oak Ridge National Laboratory
  - ❖17590.0 TFlop/s (17.59 PFLOPS)

  $17.59 \times 10^{15} \approx 10^{16.24} \approx 2^{54}$ calculations per second
- 100 years $\approx 2^{32}$ seconds
- 100 year's calculations: $2^{54} \times 2^{32} = 2^{86}$

What if 1000000 Such Supercomputers?

- One supercomputer: $17.59 \times 10^{15} \approx 10^{16.24}$
- 1000000 (10^6) such computers
  - ❖$10^{22.64}$ calculations per second

  $\approx 2^{75.22}$
- 100 years: 2^{32} seconds
- 100 years' calculations = ?

  $2^{75.22} \times 2^{32} \leq 2^{108}$

What if 1 billion Such Supercomputers?

- One supercomputer: $17.59 \times 10^{15} \approx 10^{16.24} \approx 2^{54}$ calculations per second
- 1000000000 ($10^9 \approx 2^{29.9}$) such computers

  $2^{54} \times 2^{29.9} \approx 2^{84}$ calculations per second
- 100 years: 2^{32} seconds
- How many calculations in 100 years?

  $2^{84} \times 2^{32} \approx 2^{116}$

Lessons?

Computers have computing limits

① Numbers (Intel CPU)

- # of seconds in a day? 2^{17}
- # of seconds in a year? 2^{25}
- # of seconds in 100 years? 2^{32}
- **Intel CPU** (3.45GHz) in 100 years? 2^{64}
- 1 million Intel CPU (3.45GHz) in 100 years: 2^{86}
- 1 billion Intel CPU (3.45GHz) in 100 years: 2^{94}

① Numbers (The Fastest Computer)

- # of seconds in a day? 2^{17}
- # of seconds in a year? 2^{25}
- # of seconds in 100 years? 2^{32}
- **The fastest computer** in 100 years? 2^{86}
- 1 million fastest computers in 100 years: 2^{108}
- 1 billion fastest computers in 100 years: 2^{116}

So?

- A 128-bit string 0110101010101…

  – Randomly generated

- **How many** tries does it take to guess it correctly?

  – On average: 2^{127}

- How long will it take for these tries?
  – One billion **Intel CPU** (3.45GHz)? 800 billion years
  – One billion fastest computers? 200 thousand years

Space

- 1K bytes
- 1M bytes
- 1G bytes
- 1Tera bytes (TB)
- 1Peta bytes (PB)
- 1 exabyte (EB)
- 1 zettabyte (ZB)
- 1 yottabyte (YB)

- 2^{10}
- 2^{20}
- 2^{30}
- 2^{40}
- 2^{50}
- 2^{60}
- 2^{70}
- 2^{80}

4 terabytes = 2^{42}

120 PB (memory)
≈ $\mathbf{2^{57}}$

NSA data center in Utah: 5 zettabytes (storage)

Passwords vs. a Strong Key

- Assume that password length = 8, how many passwords can we have?
  - The possible alphanumeric set size is (26 + 26 + 10 = 62), thus the possible combination size is 62^8 = 218340105584896 ($\approx \mathbf{2^{48}}$)
  - {`!@#$%^&*()~';,./:"<>?|{}[]\} = 90, thus the total combinations are at most 127^8

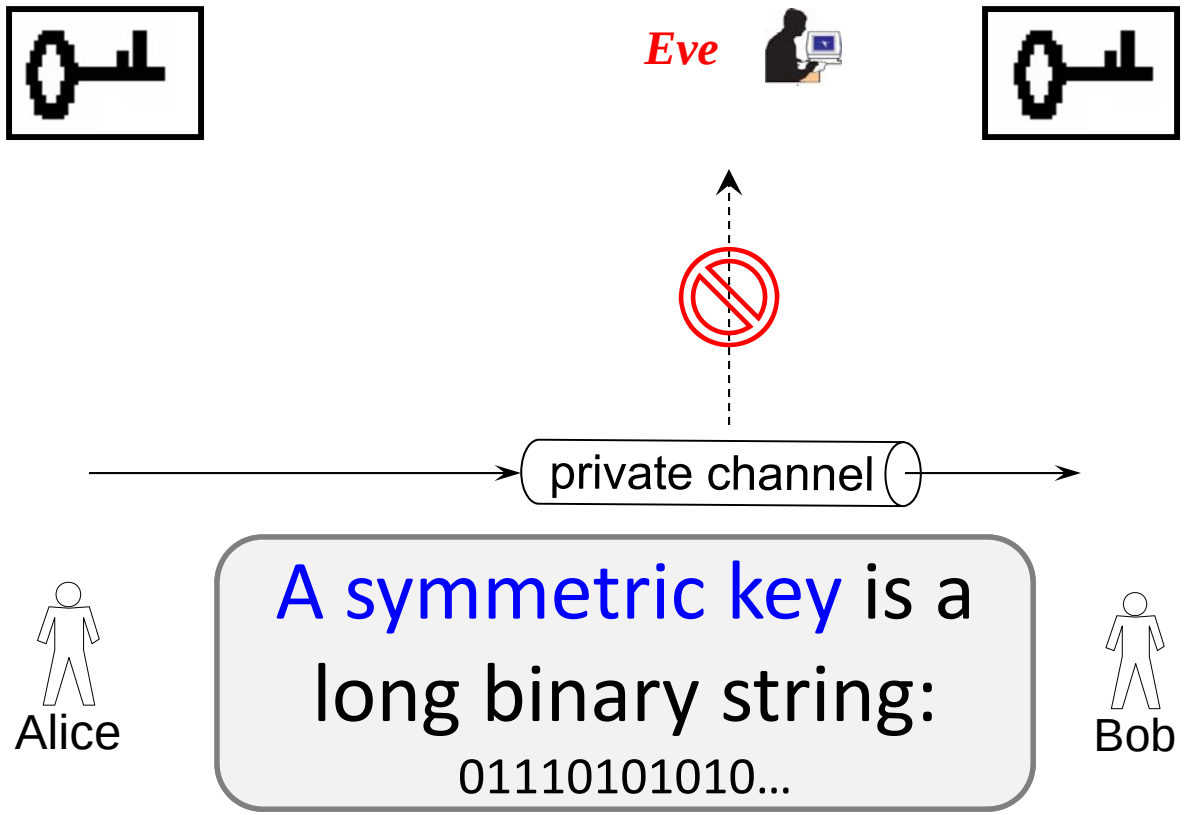
    $\approx \mathbf{2^{56}}$

Roughly 4 seconds for the fastest computer

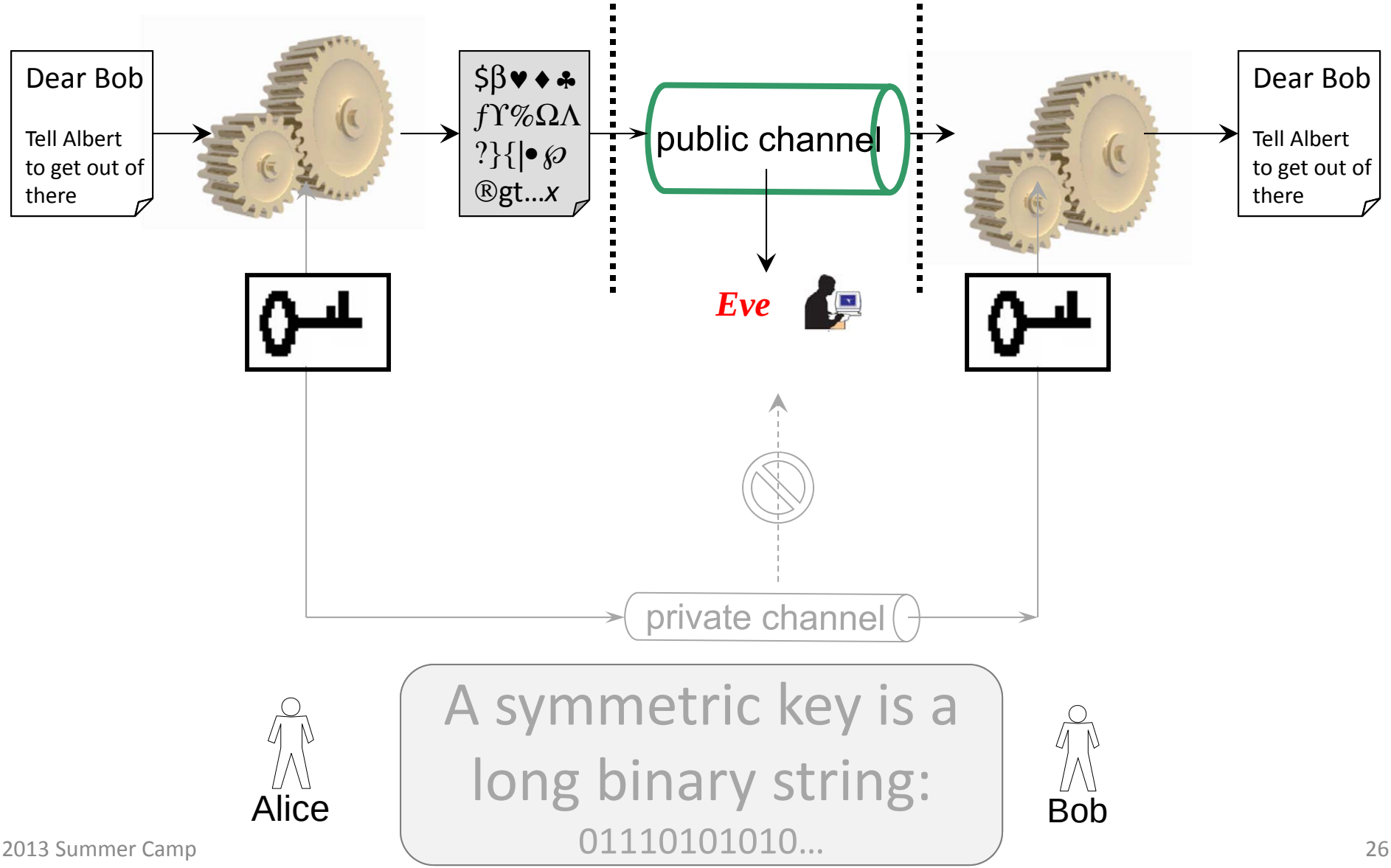
Road Map

- The data confidentiality problem
- Theory
  - Numbers
  - Encryption
  - Digital signature
  - Cryptographic hashing
  - Digital certificates and PKI
- Tie everything together: HTTPS

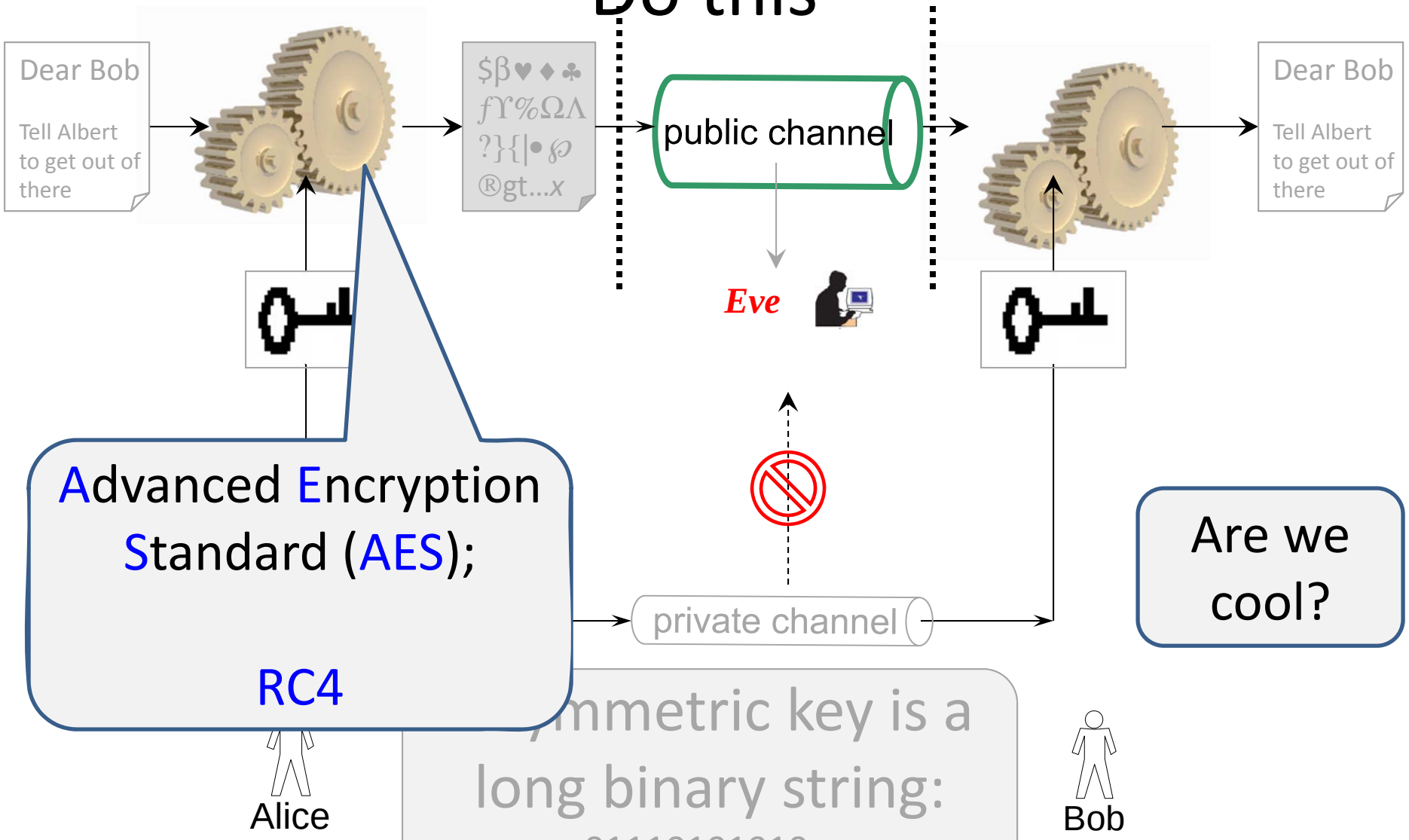
Symmetric Key Encryption



Symmetric Key Encryption

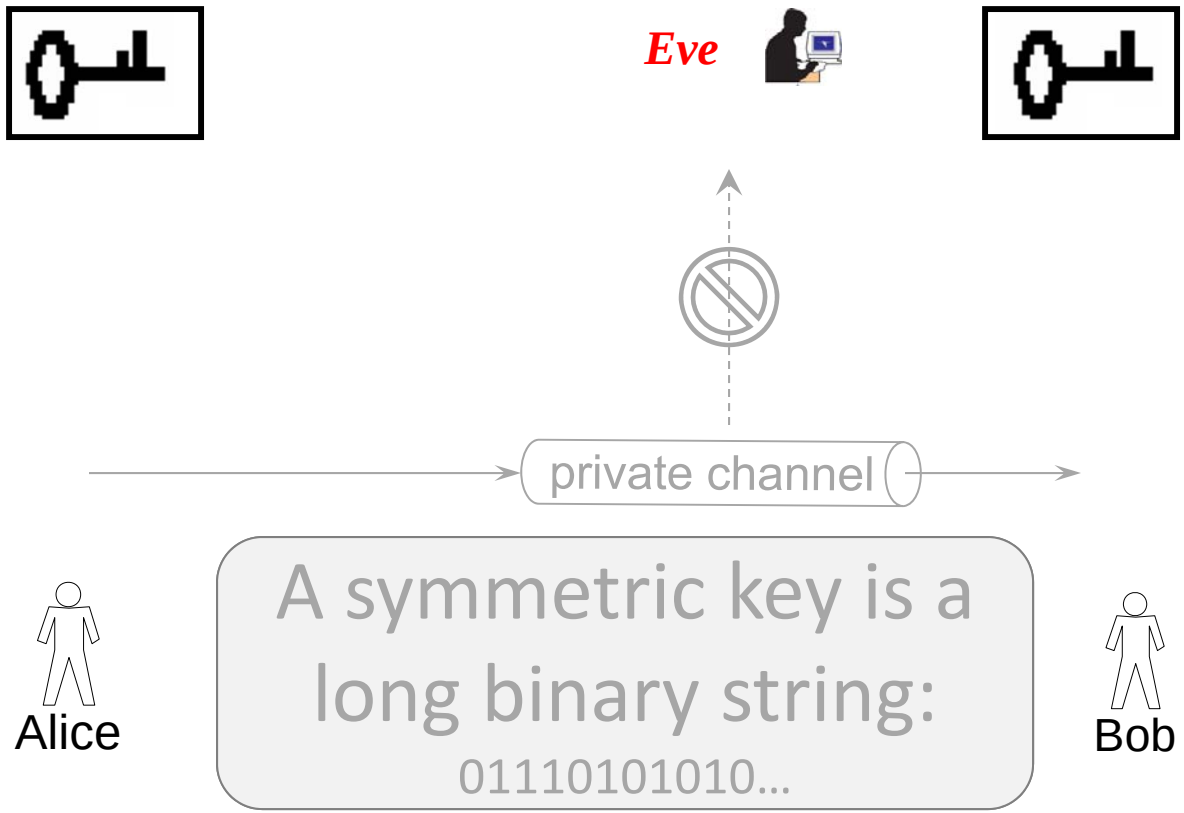


After 2000 years, We Know How to Do this

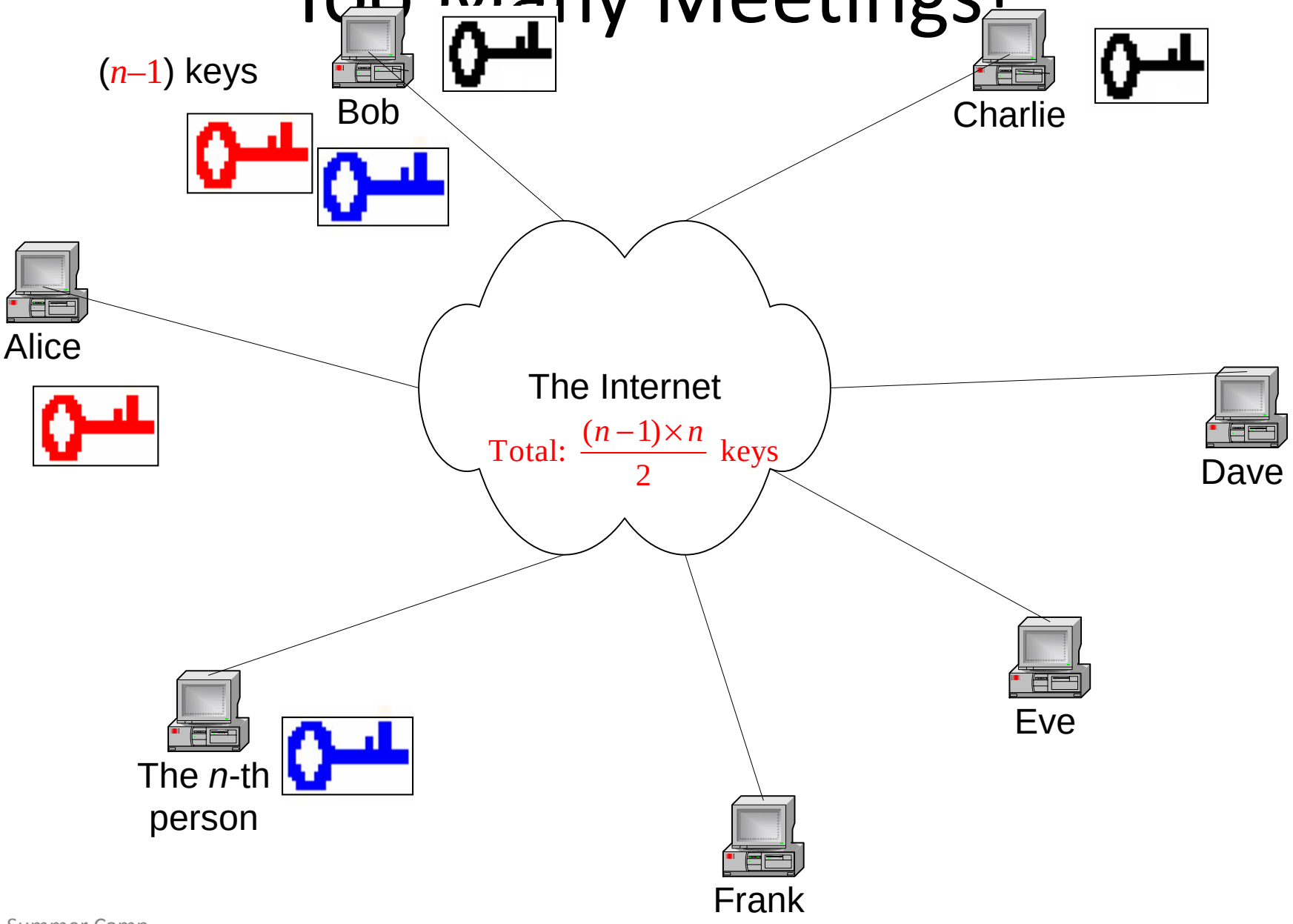


Symmetric key is a long binary string:
01110101010...

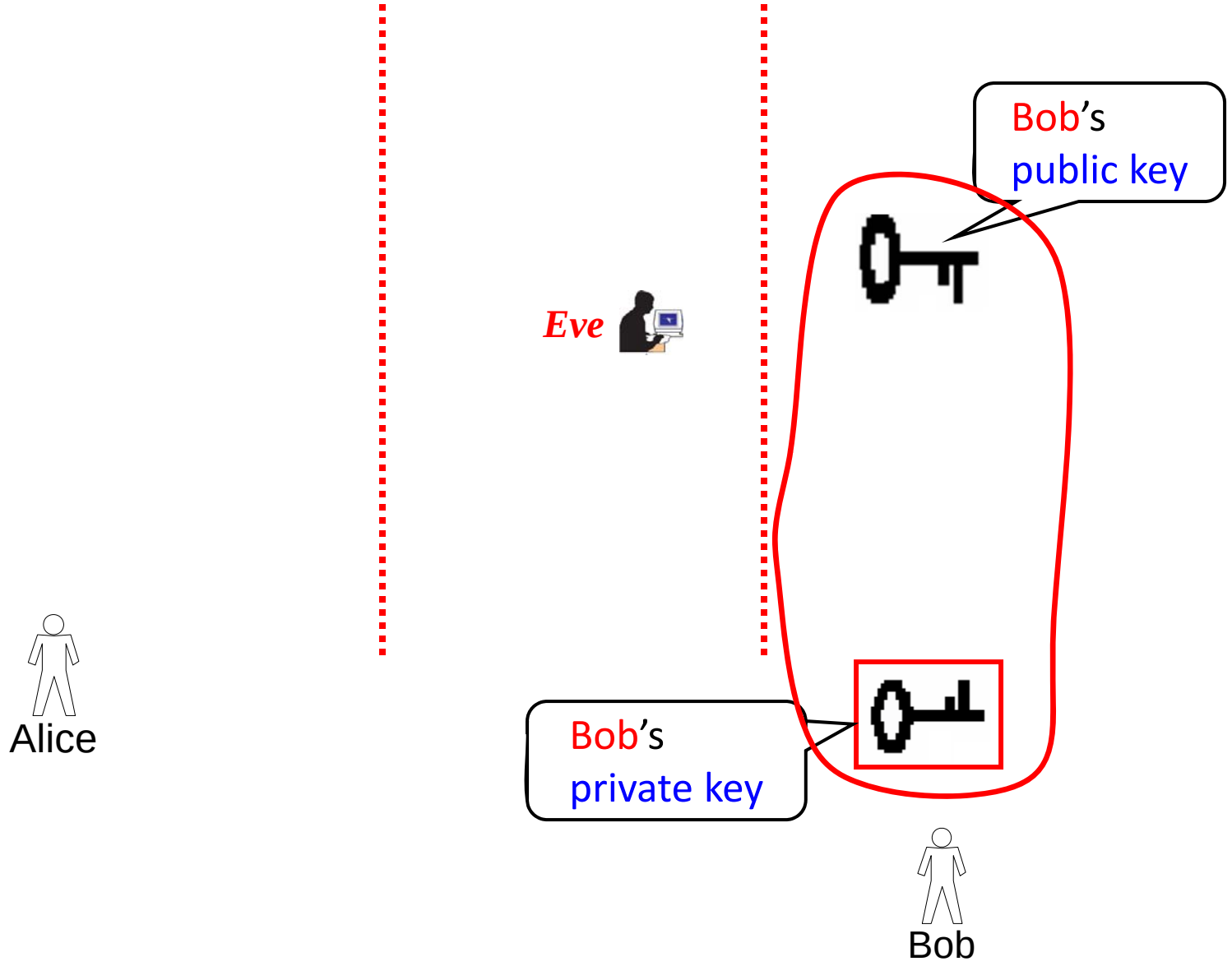
Personal Meetings?



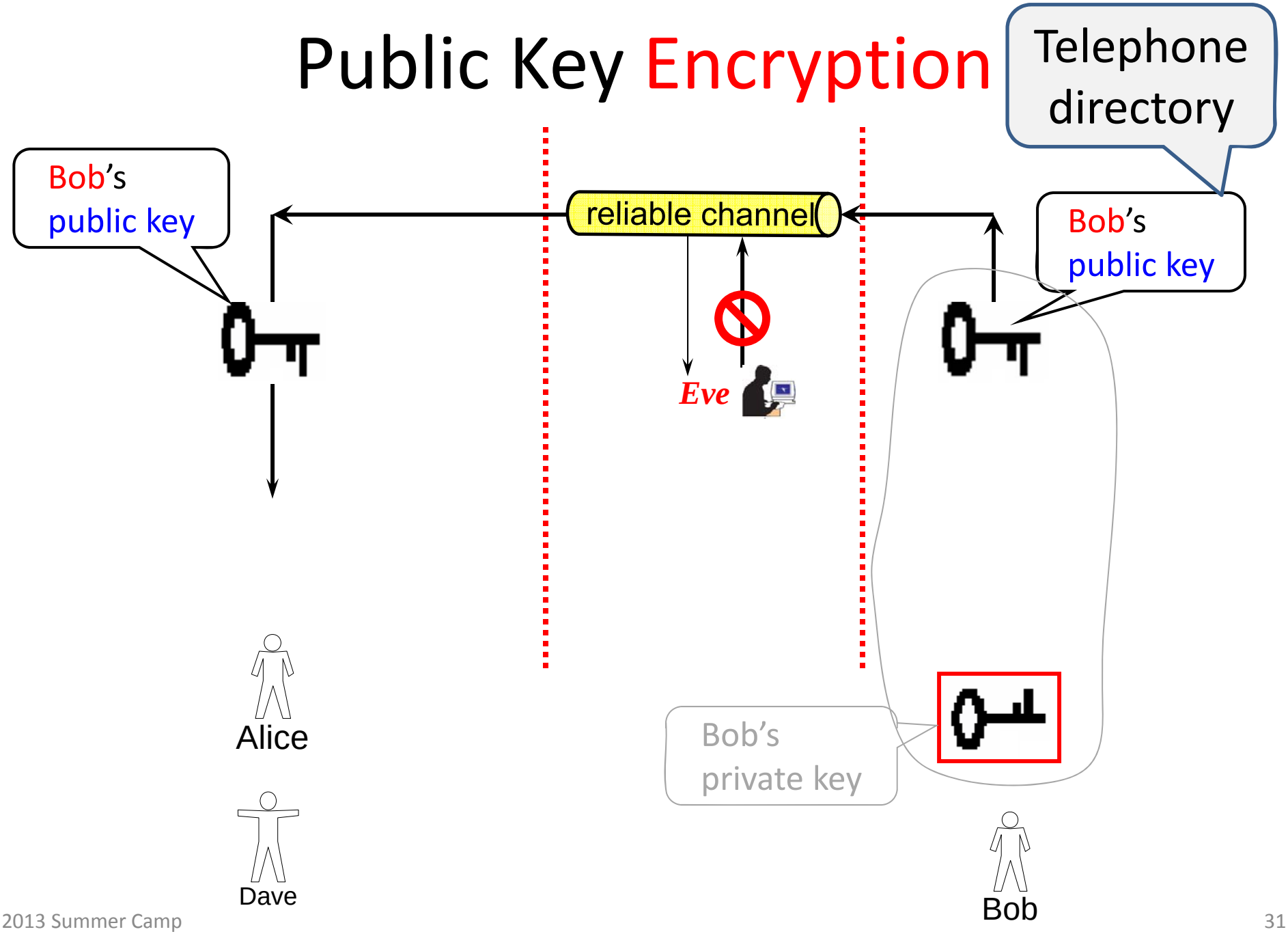
Too Many Meetings!



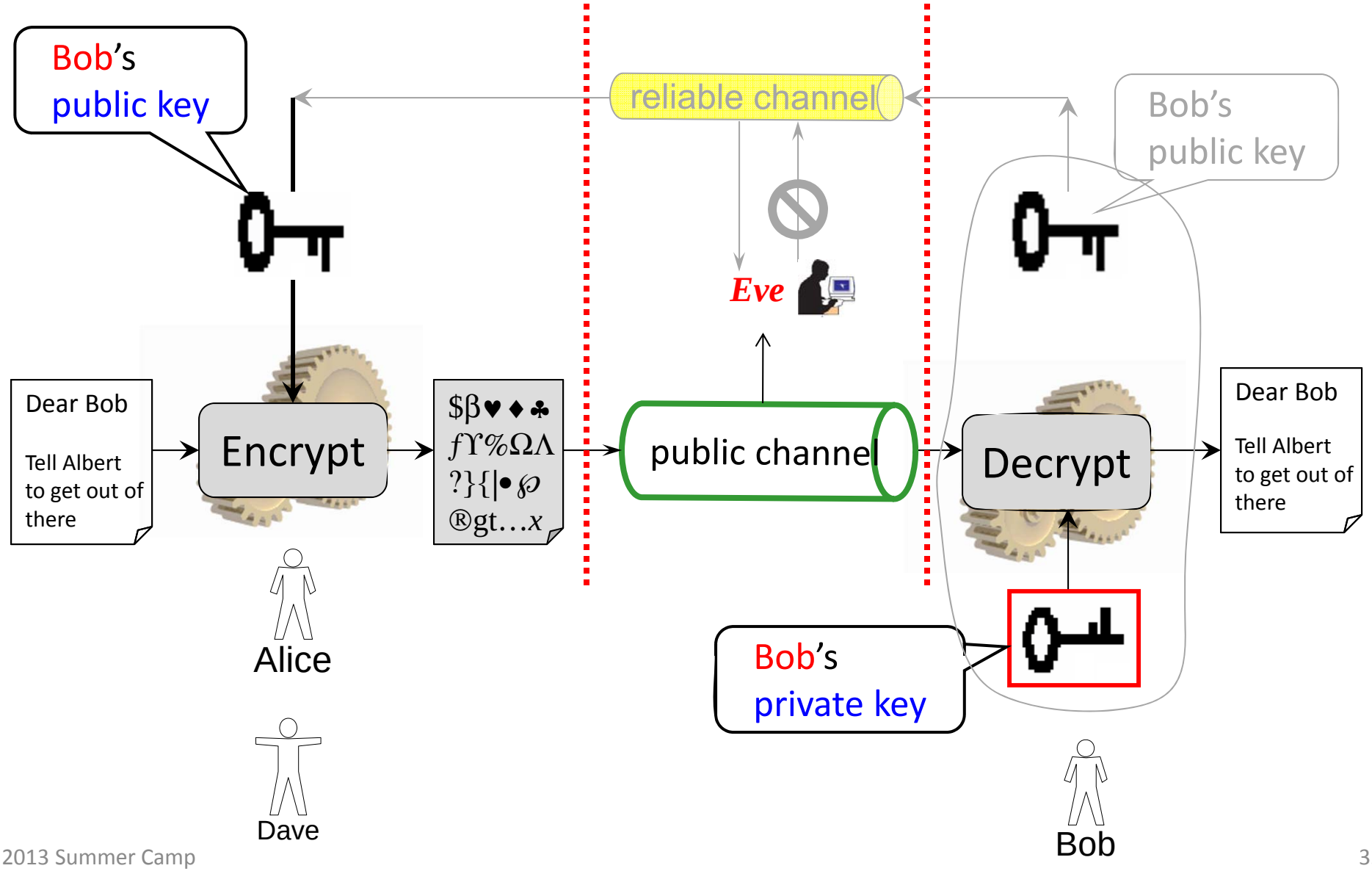
Public Key Encryption (after 1970s)



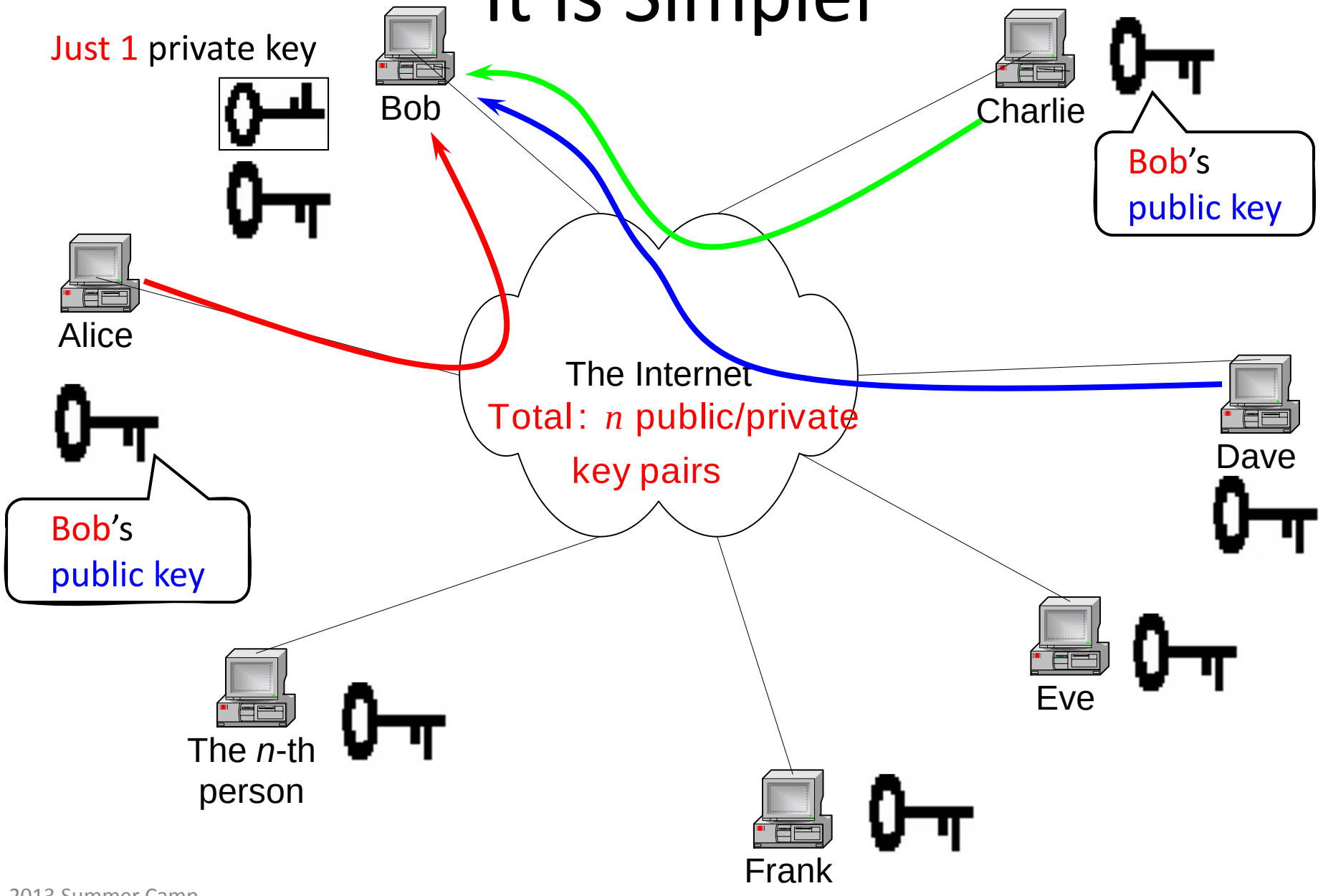
Public Key Encryption



Public Key Encryption



It is Simpler



Algorithm Buzzwords

- Symmetric key encryption algorithms
  - Advanced Encryption Standard (AES)
  - RC4 (Ron's Cipher 4)
- Public-key encryption algorithms
  - RSA: Rivest-Shamir-Adleman
  - Elliptic-curve encryption

Road Map

- The data confidentiality problem
- Theory
  - Numbers
  - Encryption
  - Digital signature
  - Cryptographic hashing
  - Digital certificates and PKI
- Tie everything together: HTTPS

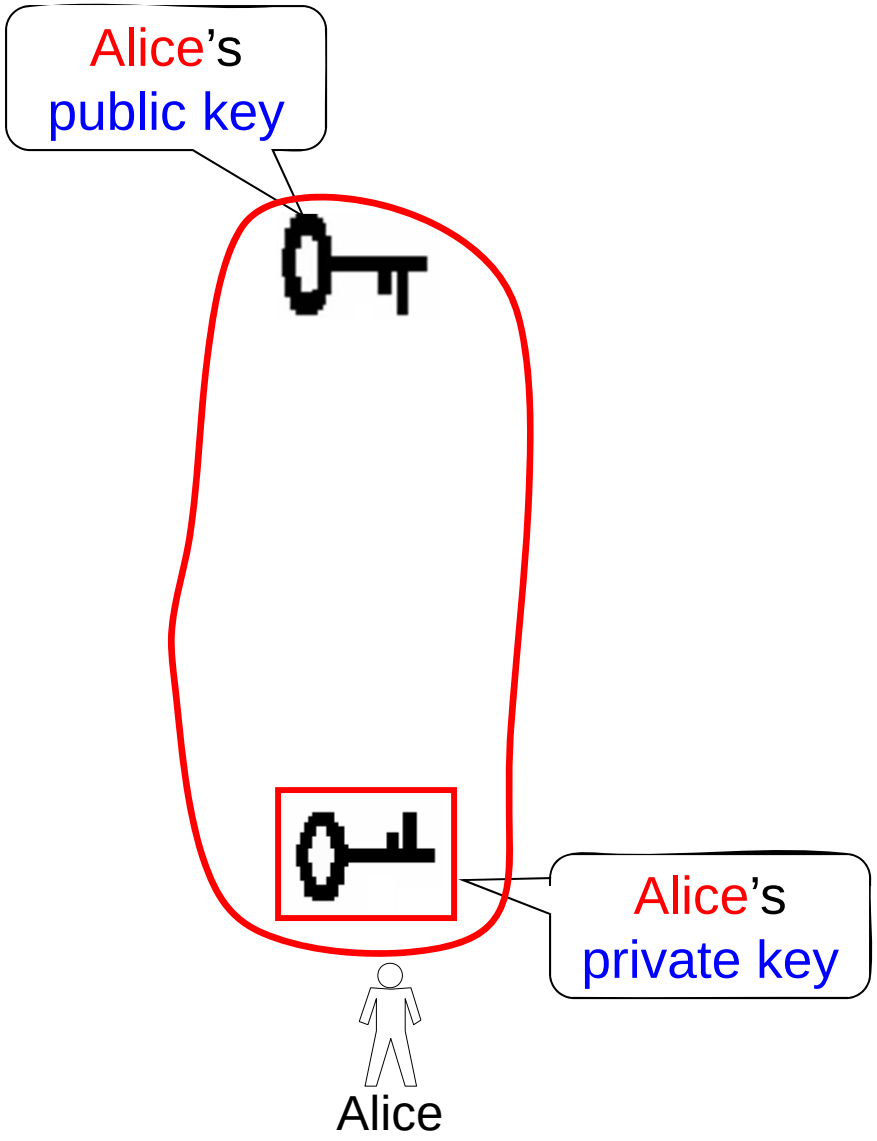
Signatures?

- Eat in a restaurant?
  - Sign your credit card payment
- Rent a house?
  - Sign the contract
- Get a car loan?
  - Sign the contract

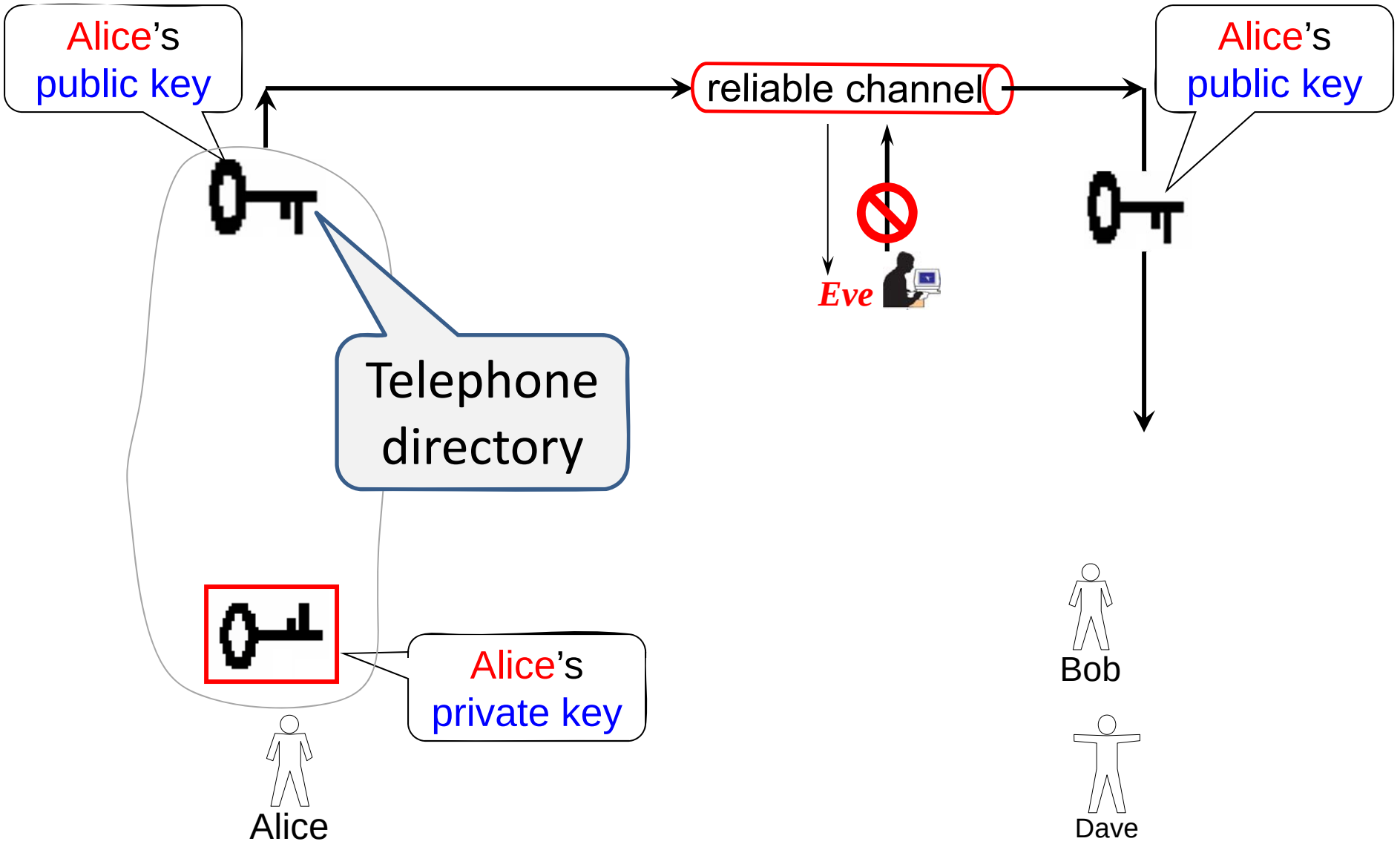
Can we implement the concept of signature in the digital world?

Handwritten signatures can be copied: does **not** work well in the digital world

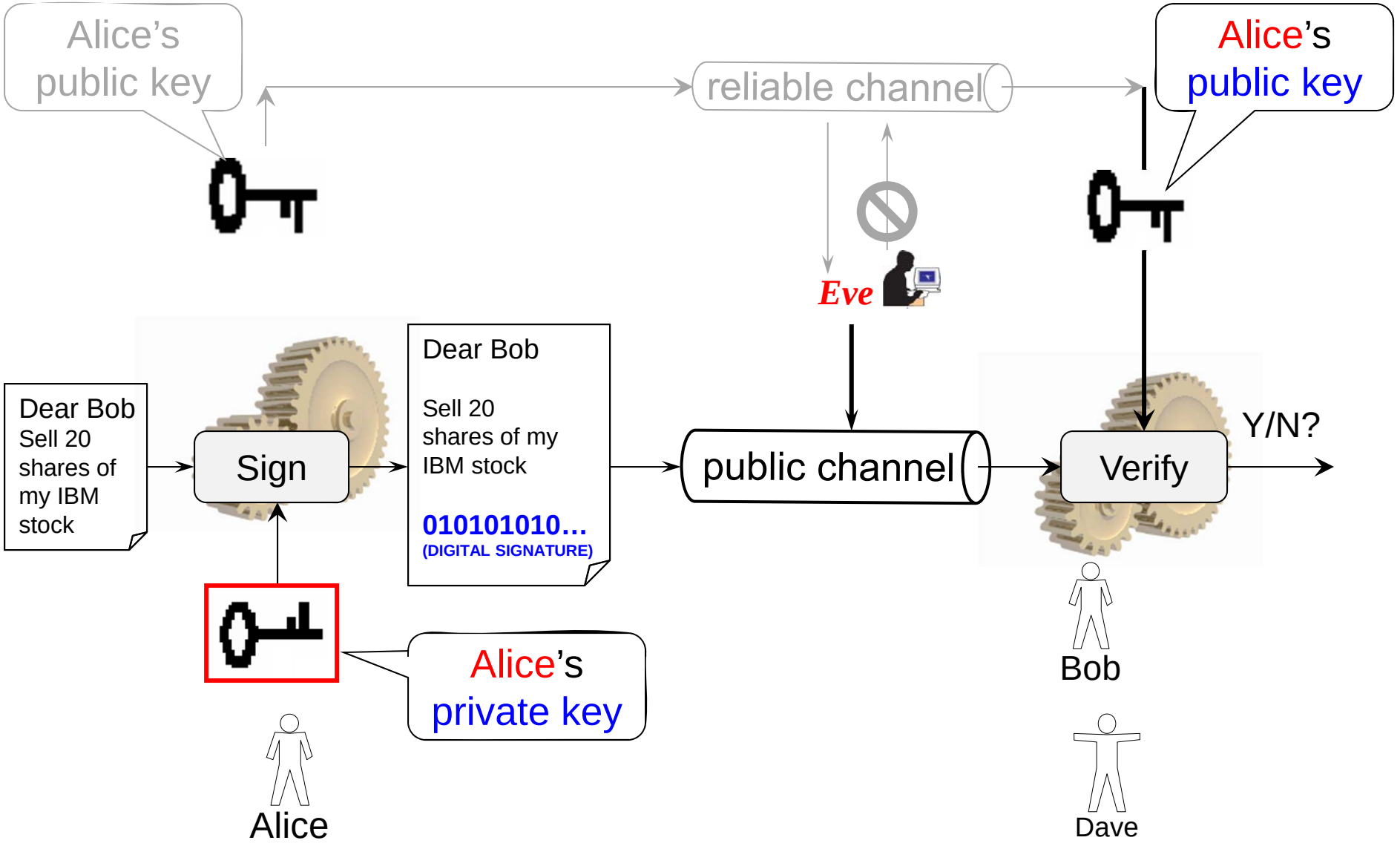
Public Key Digital Signature



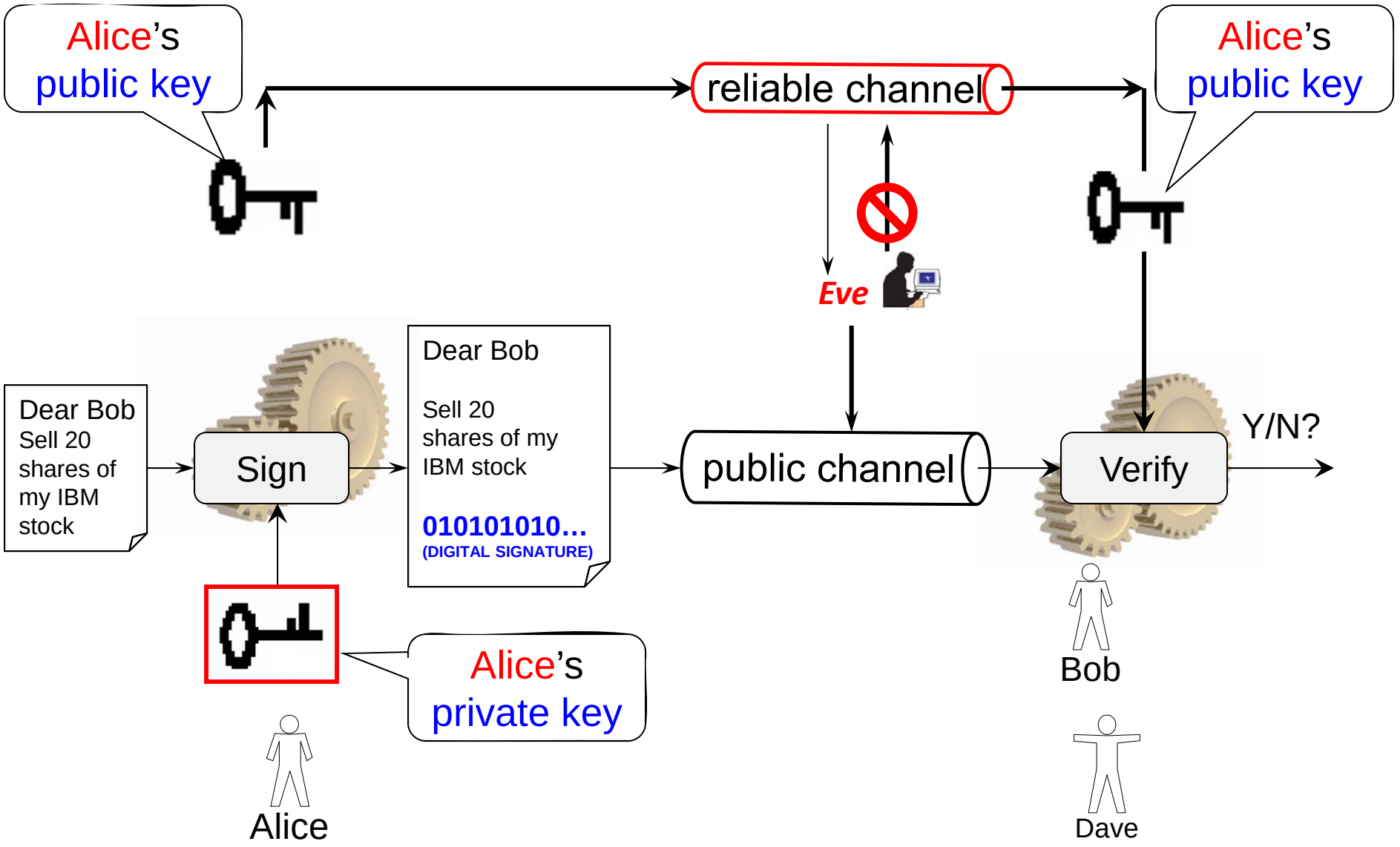
Public Key Digital Signature



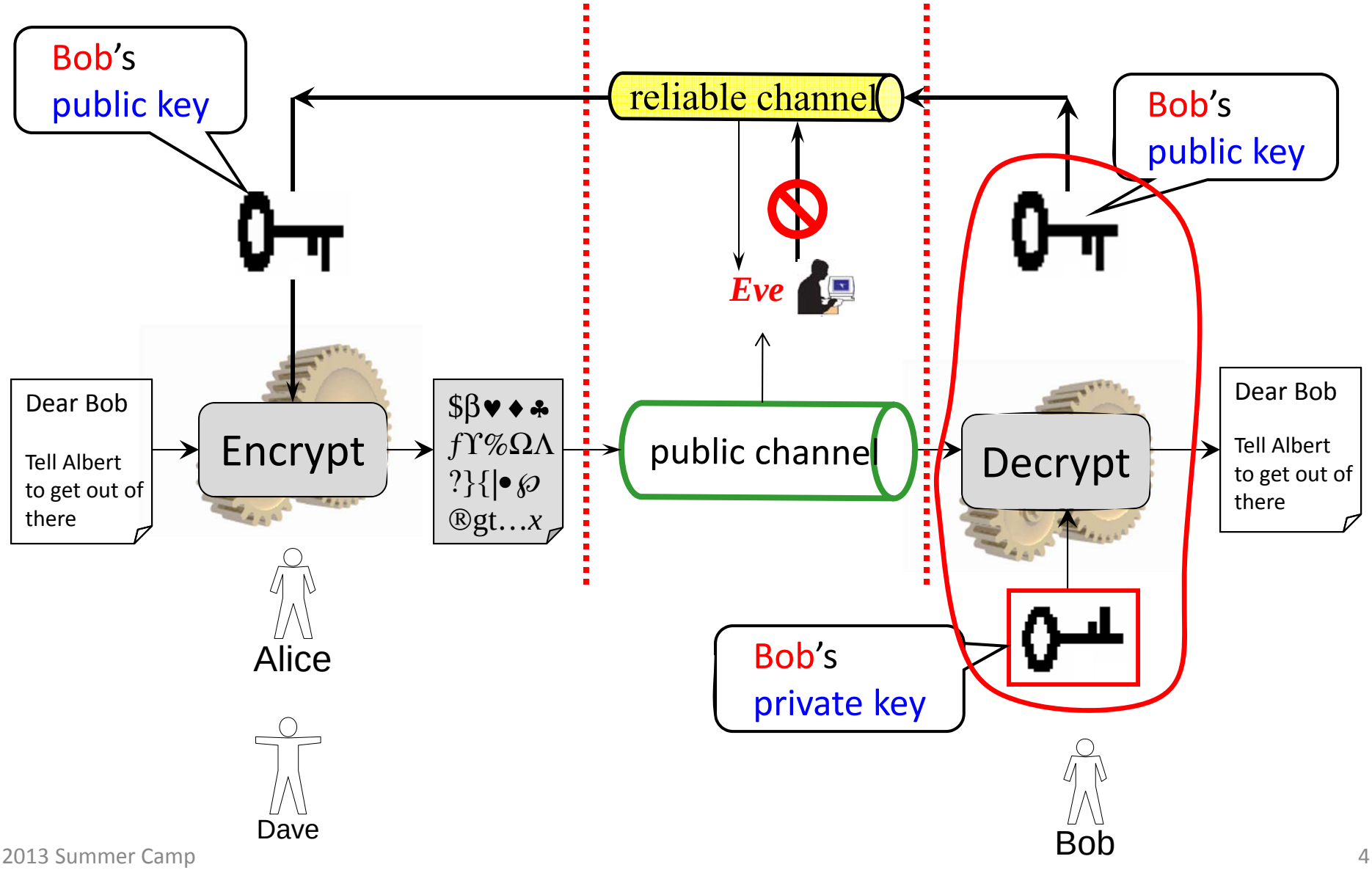
Public Key Digital Signature



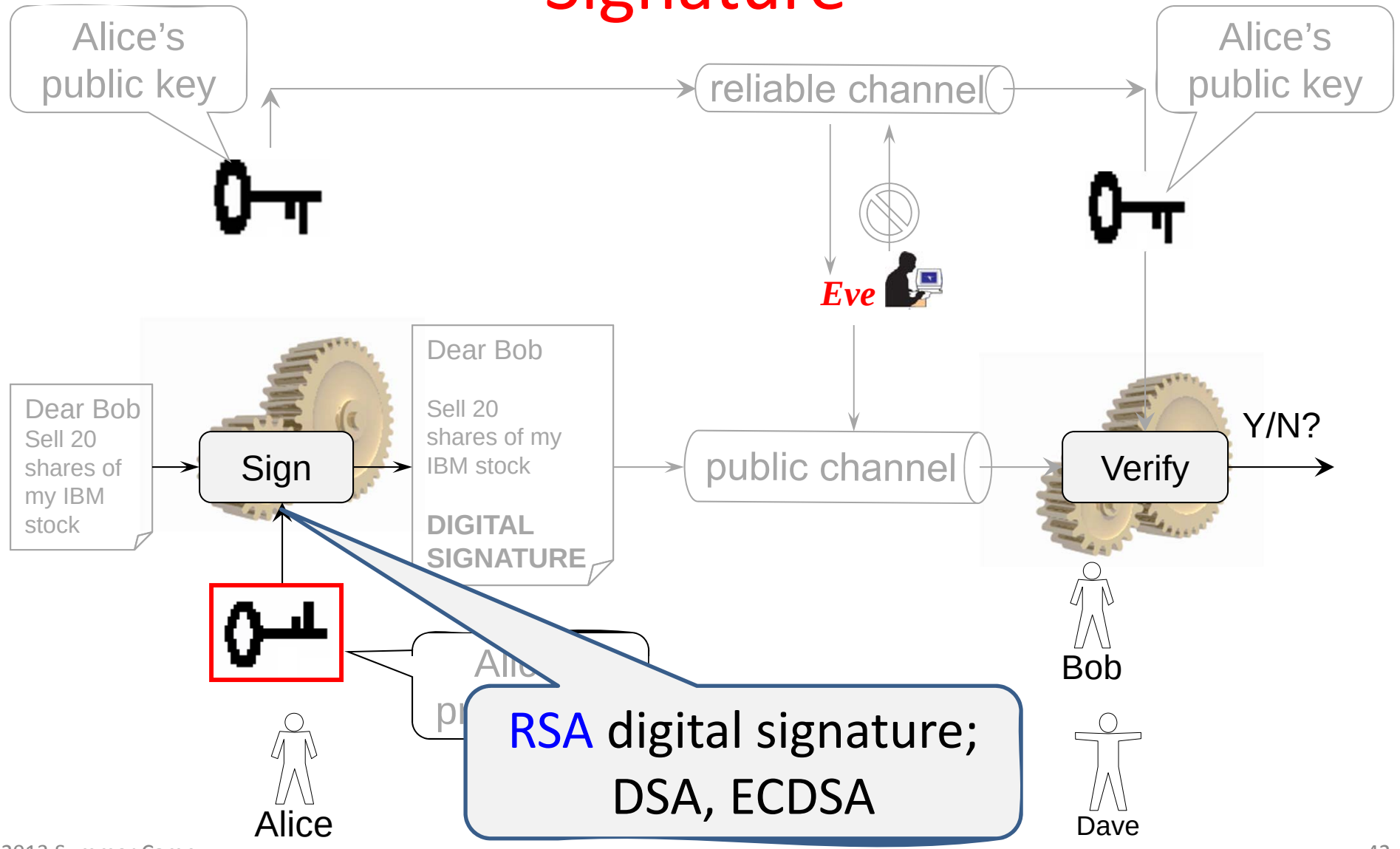
Public Key Digital Signature



Public Key Encryption



We Know How to Implement Digital Signature



Road Map

- The data confidentiality problem
- Theory
  - Numbers
  - Encryption
  - Digital signature
  - Cryptographic hashing
  - Digital certificates and PKI
- Tie everything together: HTTPS

One-way?

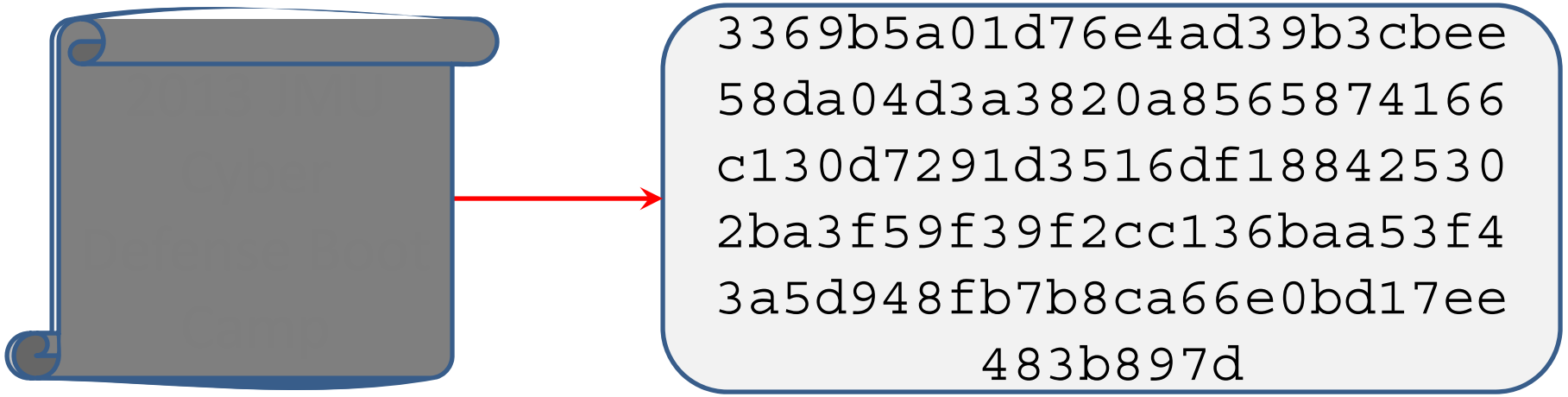
- One-way roads
  - You are not supposed to go the other way
  - But you can (break the law)

One-way Cryptographic Function?

- A big file: 4G bytes, called m
- For any function h, $y \leftarrow h(m)$
- IF for some special function h, given any value y, it is hard (for you/anybody) to find x such that $y = h(x)$
  - h is called one-way function
  - You can try, but you won't be able to computationally (**un**like one-way roads)
- Most functions are **not** one-way
- One-way functions are useful for information security

Example

- SHA512 is a cryptographic hash function

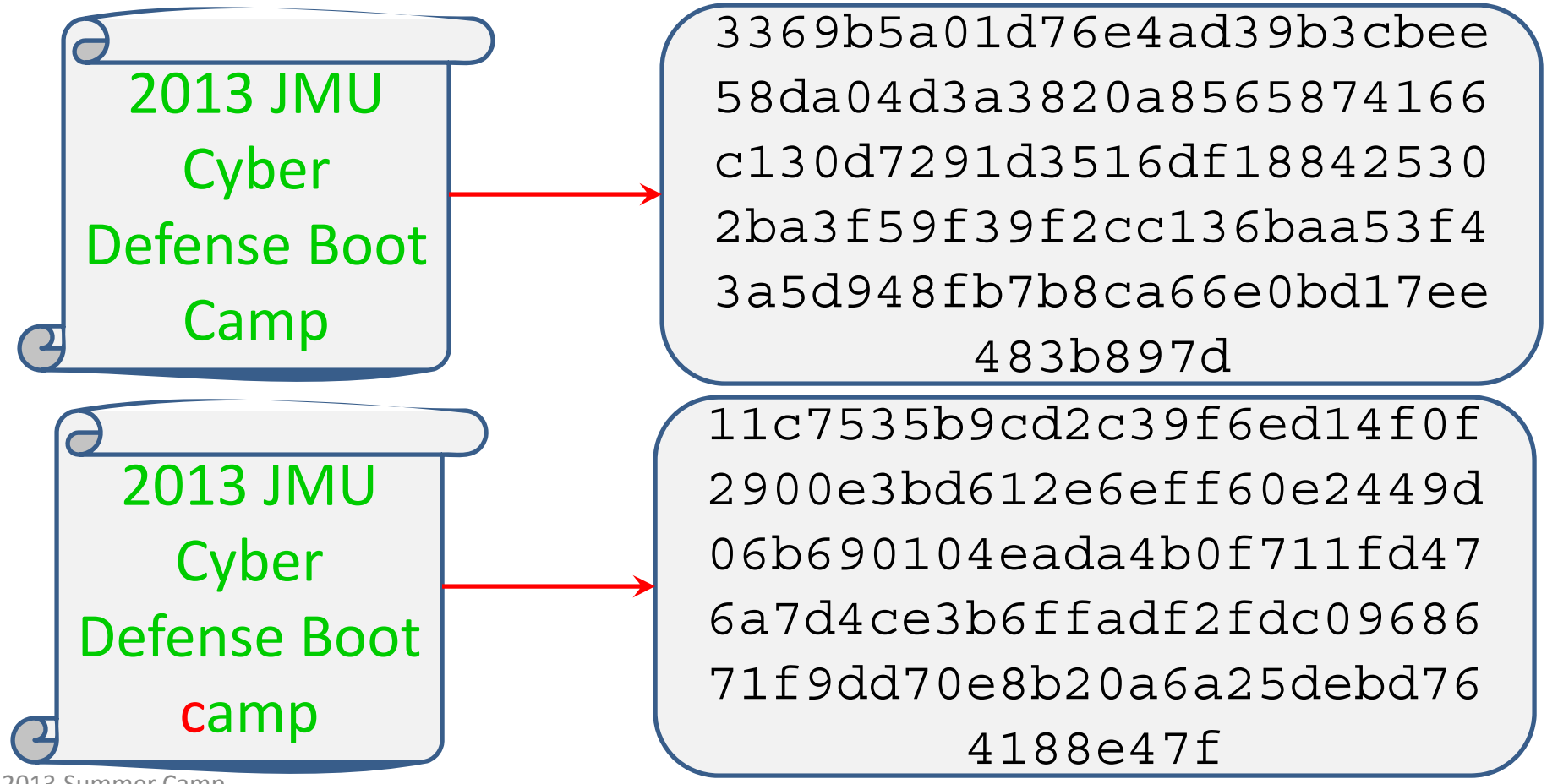


Cryptographic Hash Function

- For function h, $y \leftarrow h(m)$
- If m is always much larger than y, h is a compression function
- Form some special compression function h, it is hard to find any pair (x, y), $x \neq y$, such that $h(x) = h(y)$, h is called collision resistant
  - Not collision proof
- If h is both one-way **and** collision resistant, h is called a cryptography hash function

Example

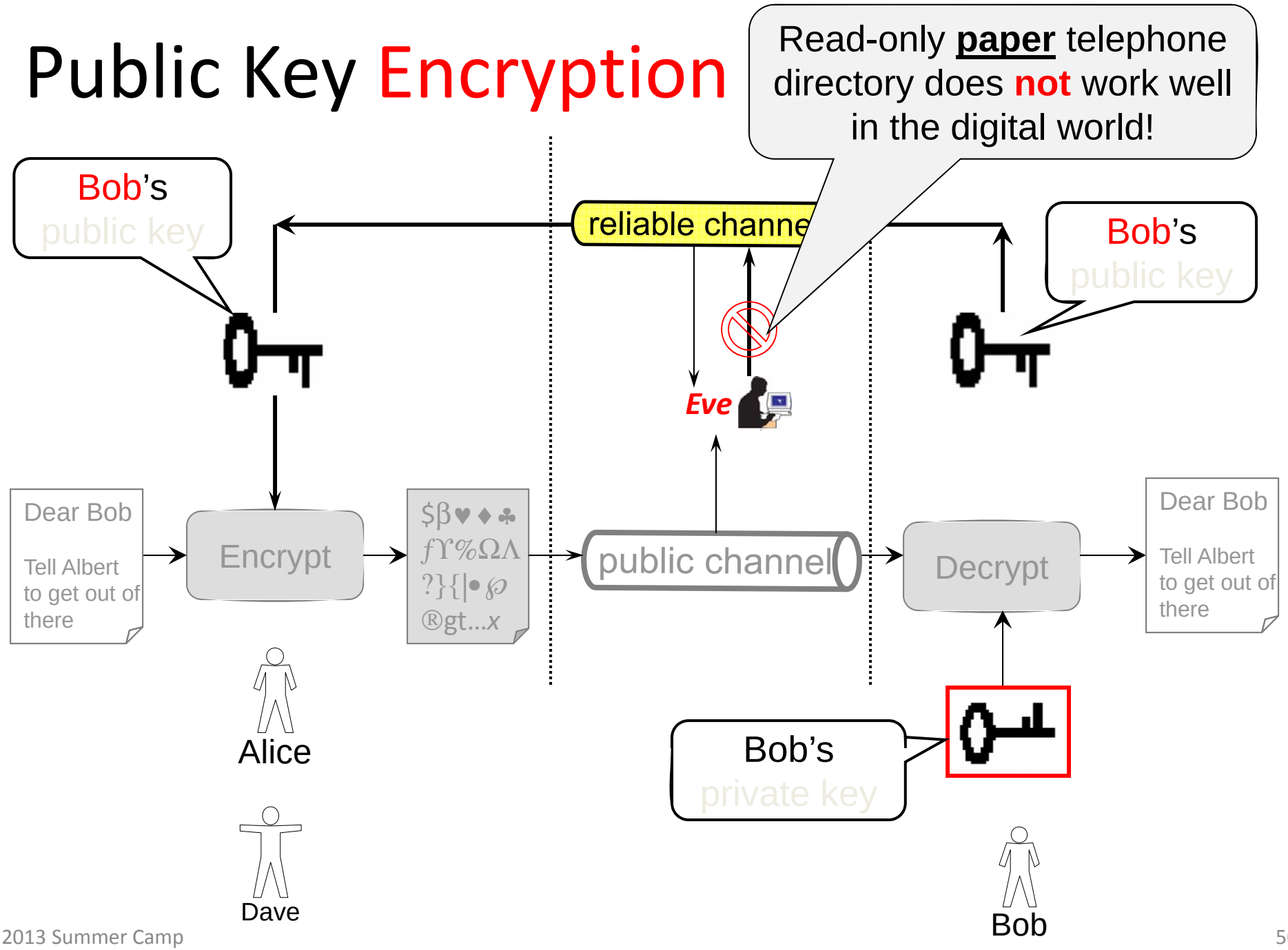
- SHA512 is a cryptographic hash function



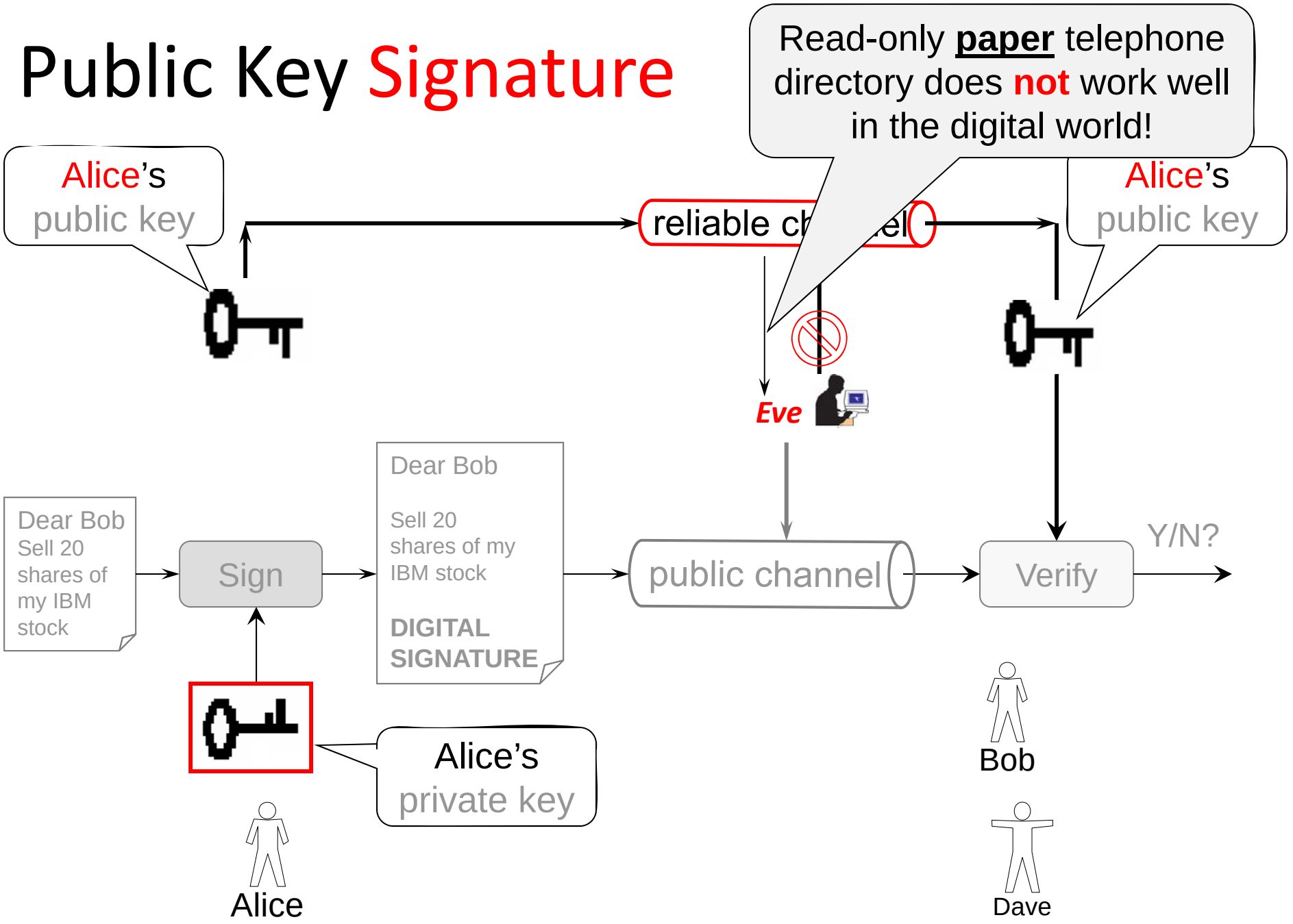
Road Map

- The data confidentiality problem
- Theory
  - Numbers
  - Encryption
  - Digital signature
  - Cryptographic hashing
  - Digital certificates and PKI
- Tie everything together: HTTPS

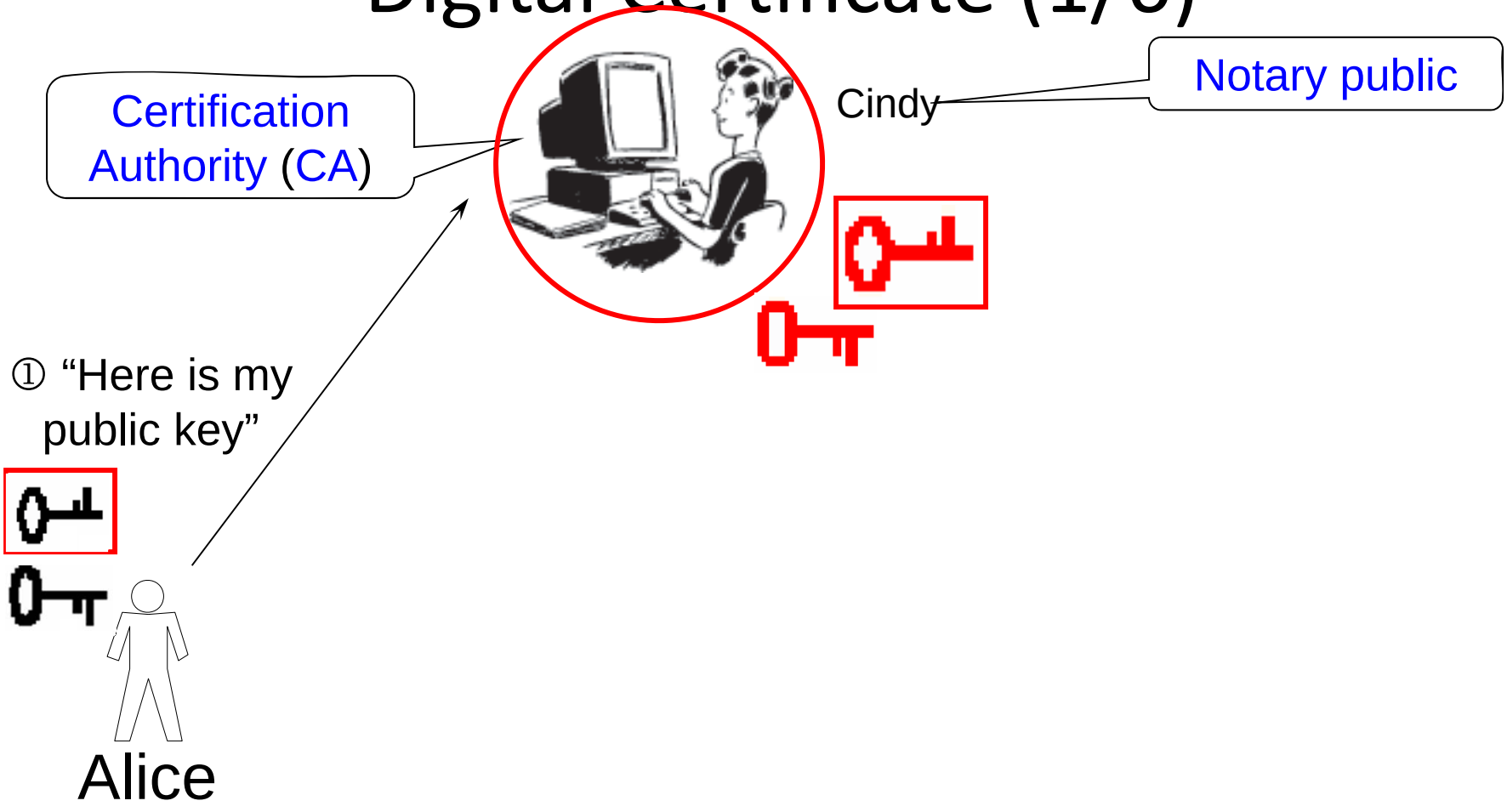
Public Key Encryption



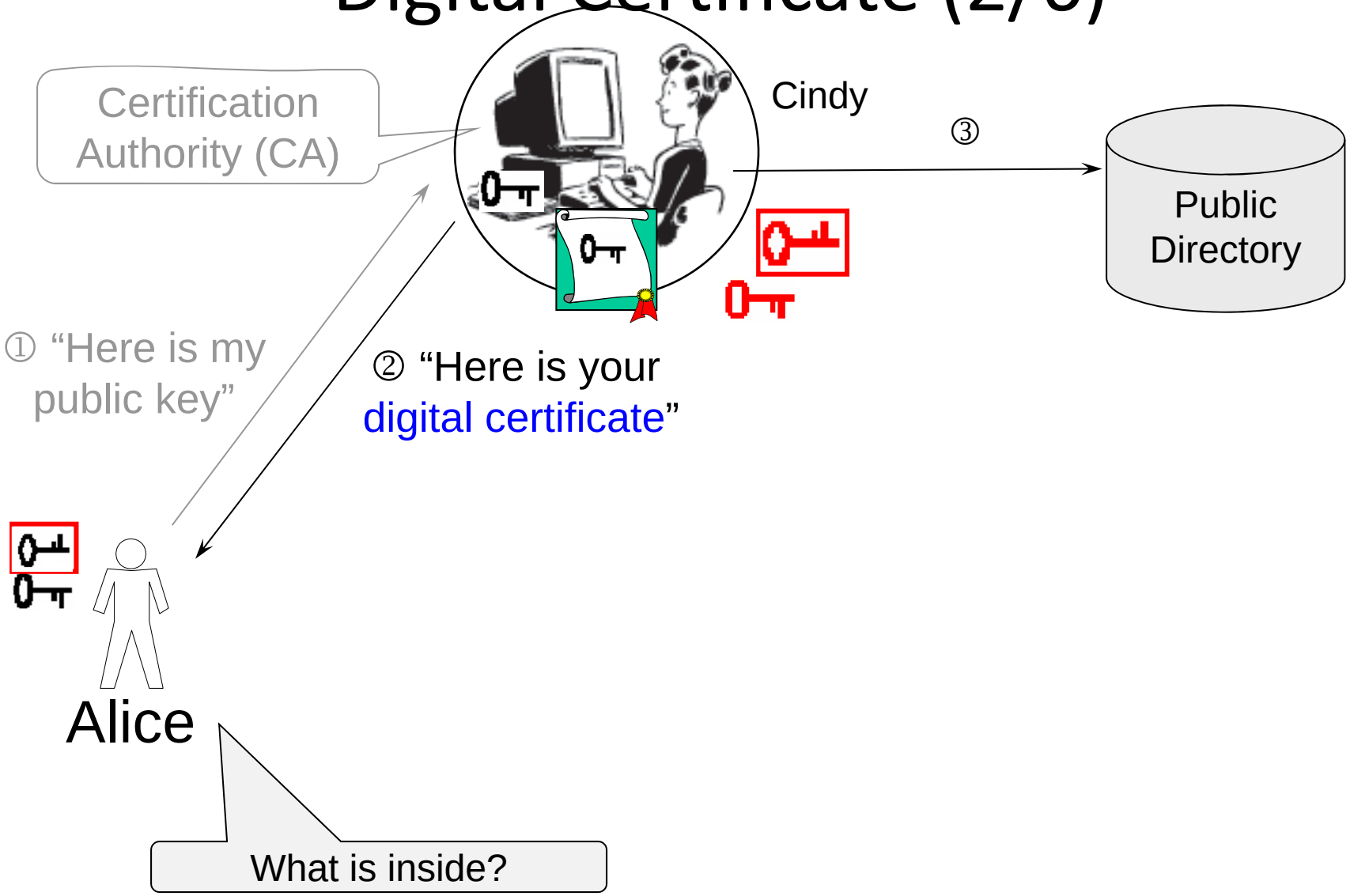
Public Key Signature



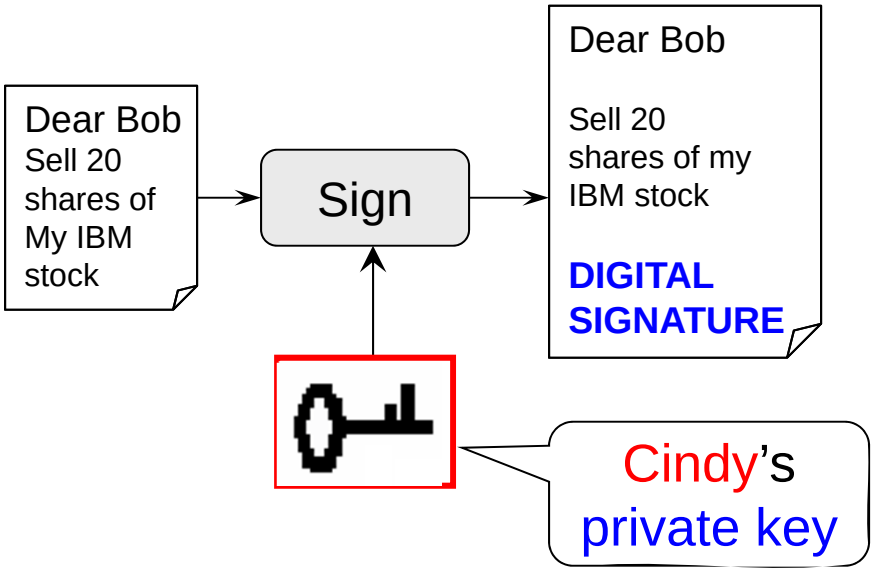
Digital Certificate (1/6)



Digital Certificate (2/6)

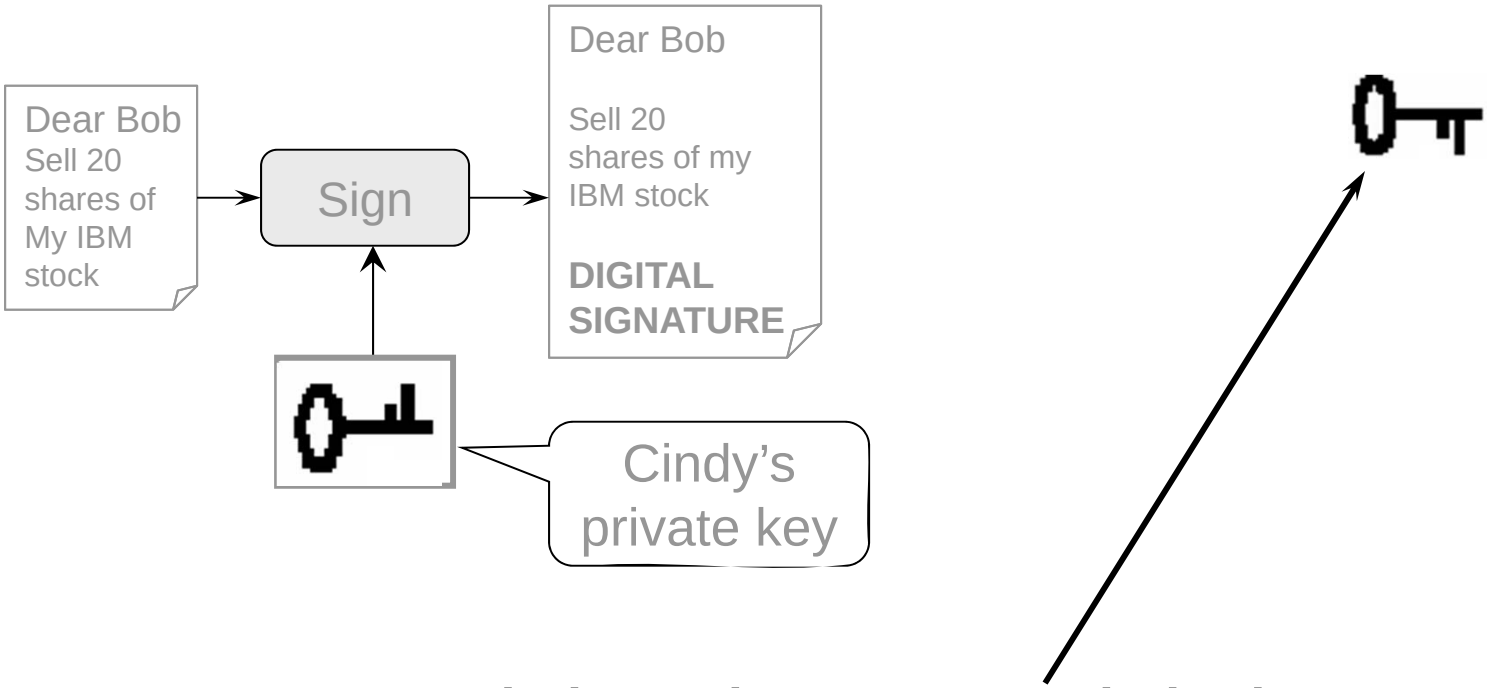


Digital Certificate (3/6)



- Questions:
  - How to verify the authenticity of the signed message?
  - What do you need to verify?

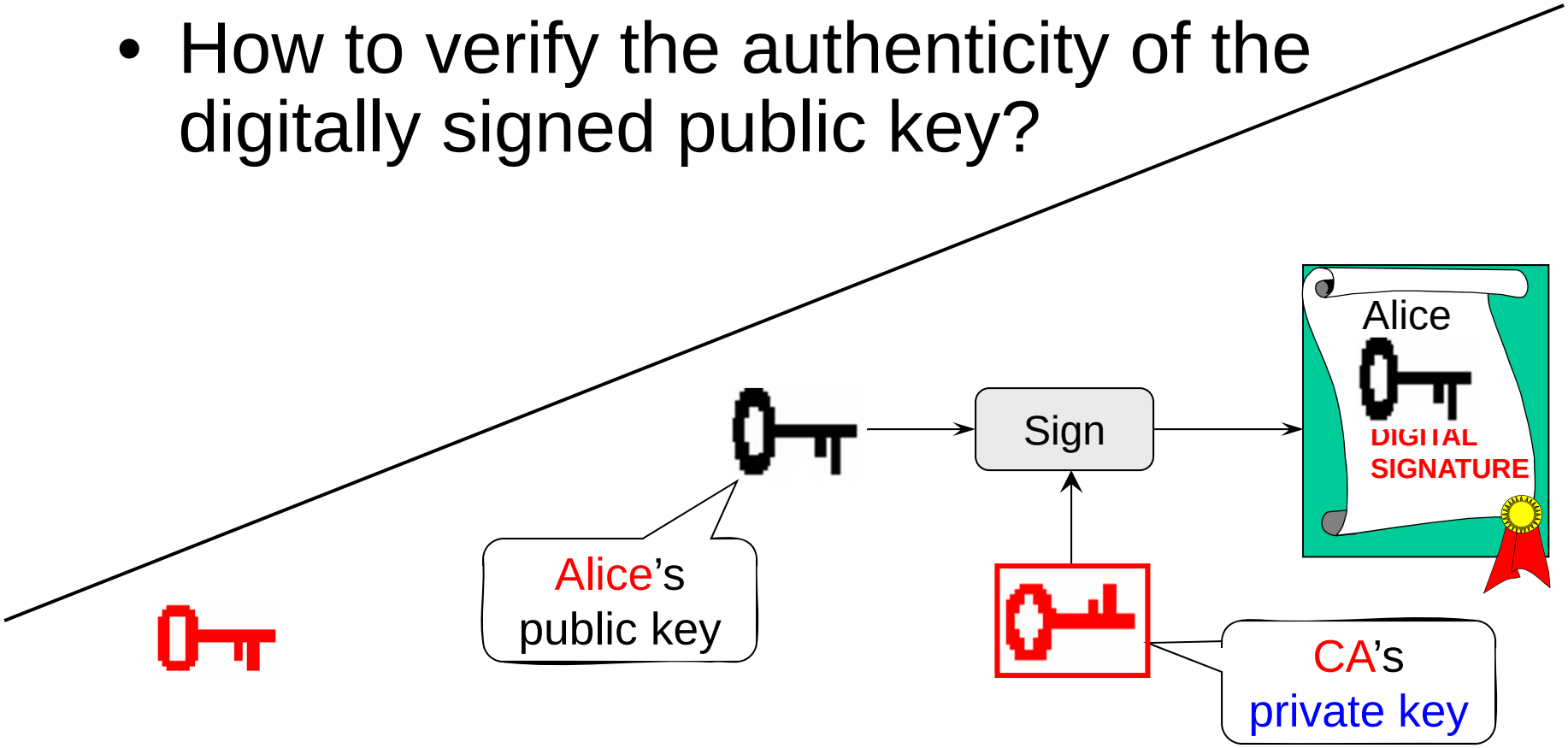
Digital Certificate (4/6)



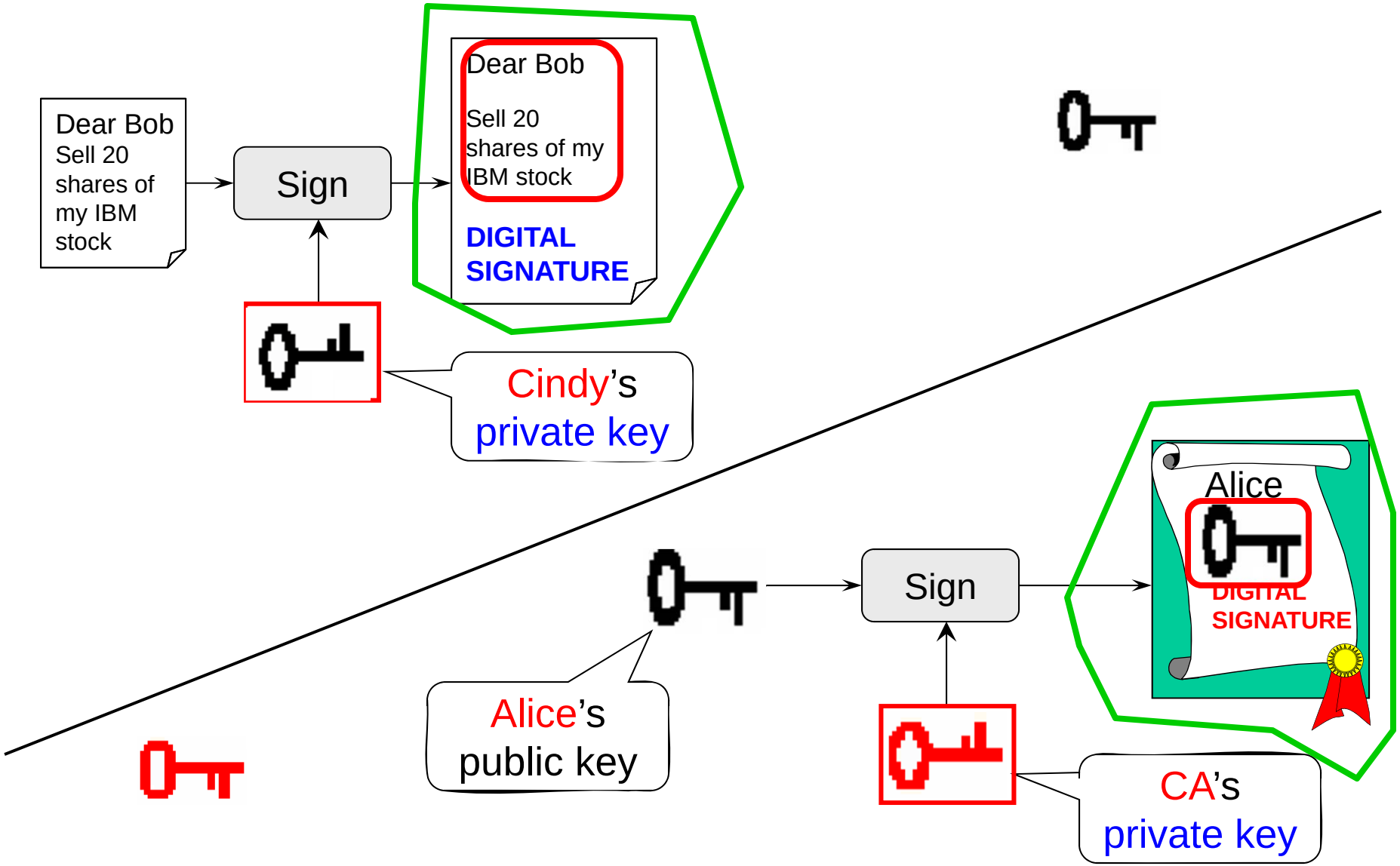
- You need the signer's public key!
- What if you mistook a bad guy's public key as the signer's public key?

Digital Certificate (5/6)

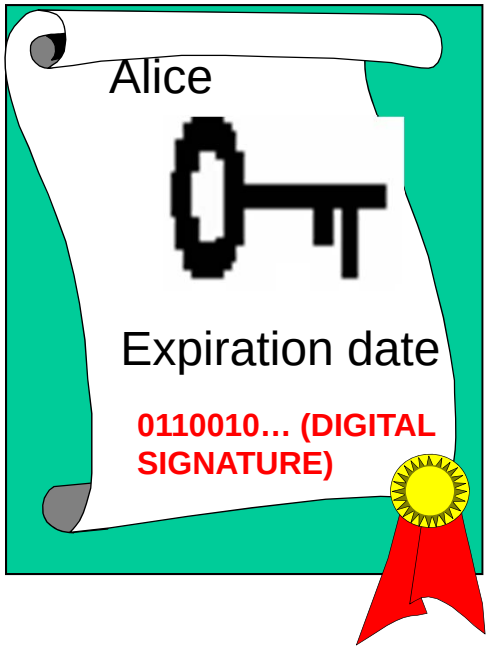
- Why not digitally sign a public key before it is distributed?
- How to verify the authenticity of the digitally signed public key?



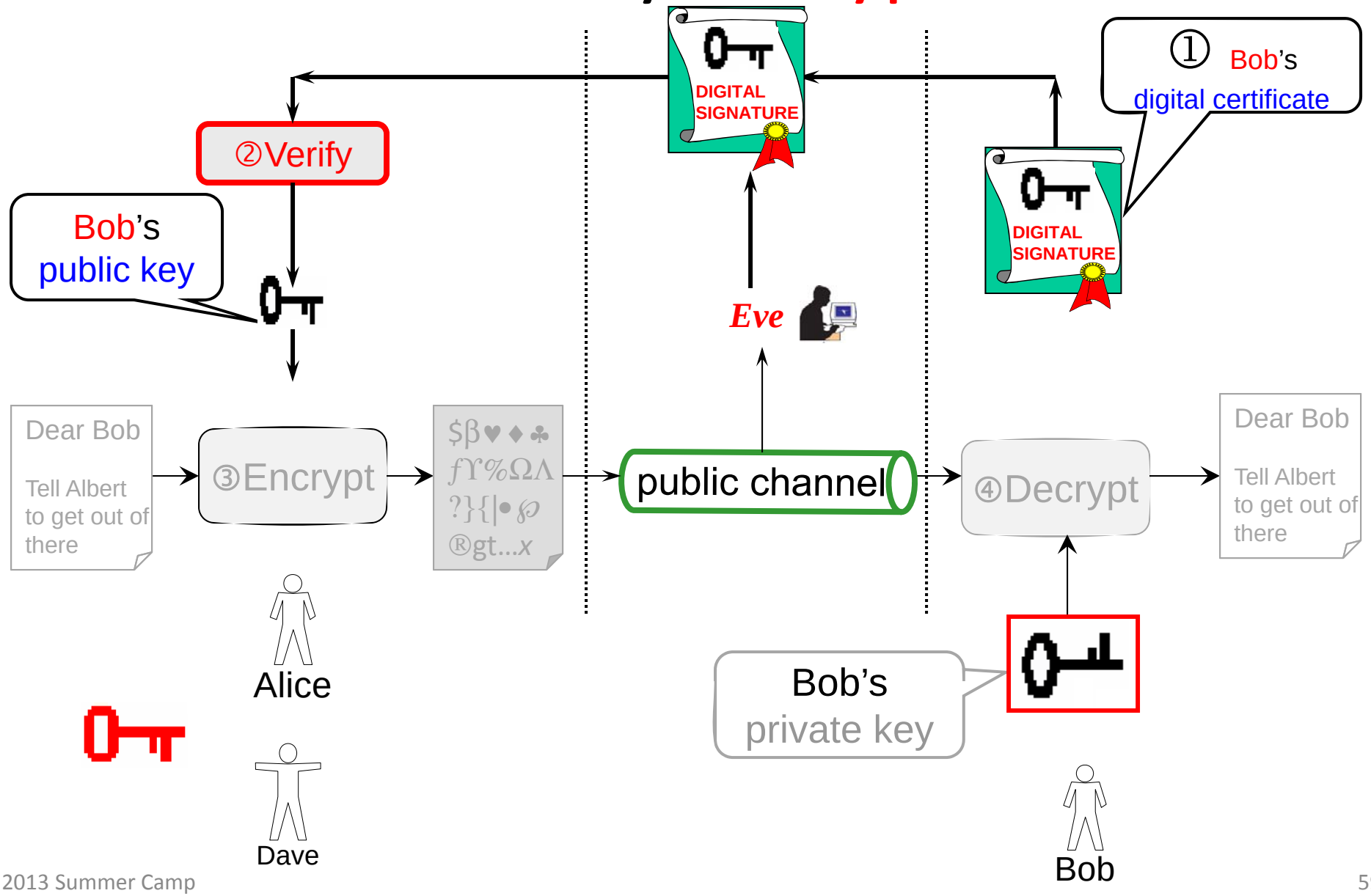
Digital Certificate (6/6)



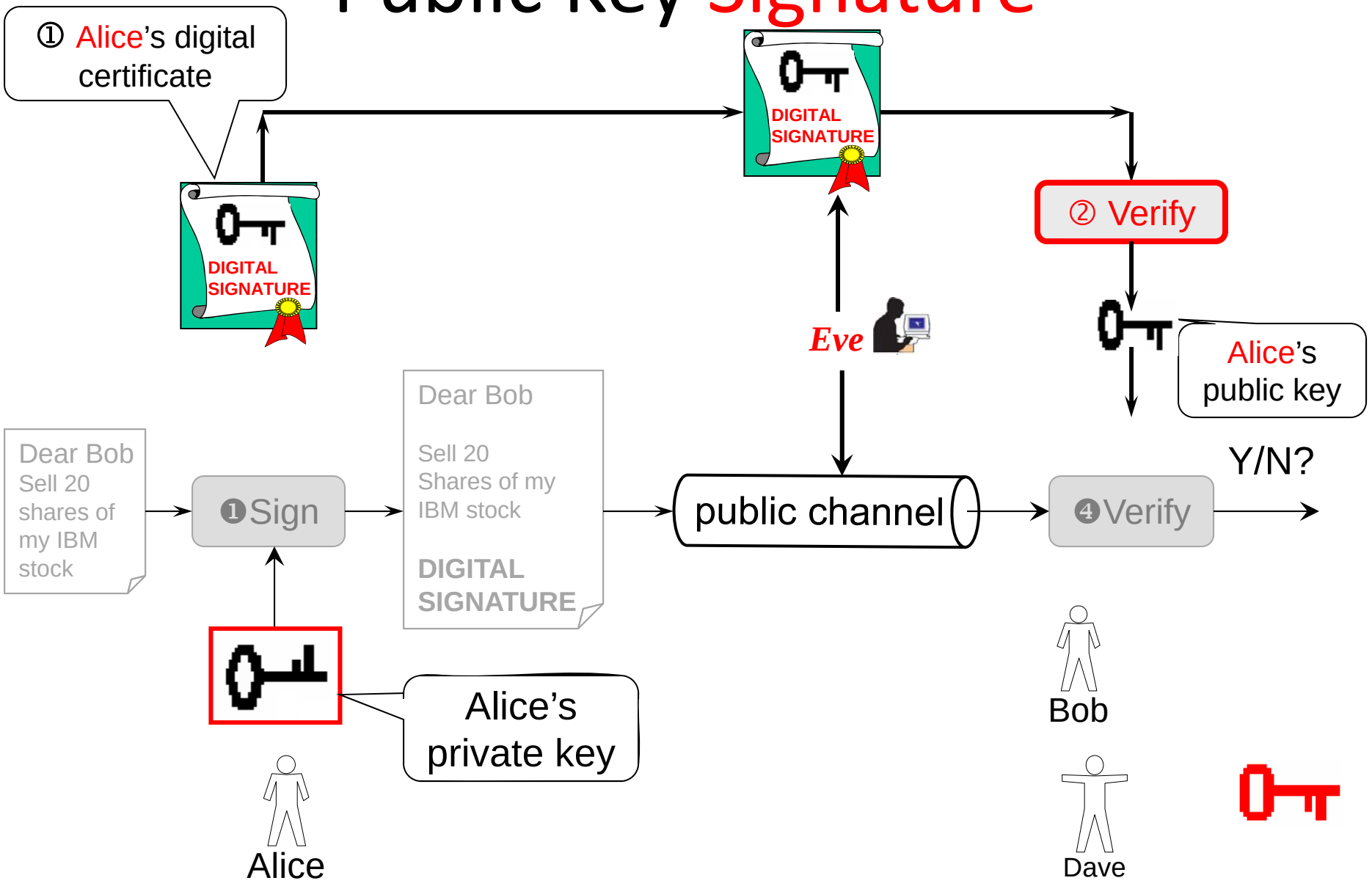
Inside a Digital Certificate



Public Key Encryption



Public Key Signature



Quotes from Don Davis

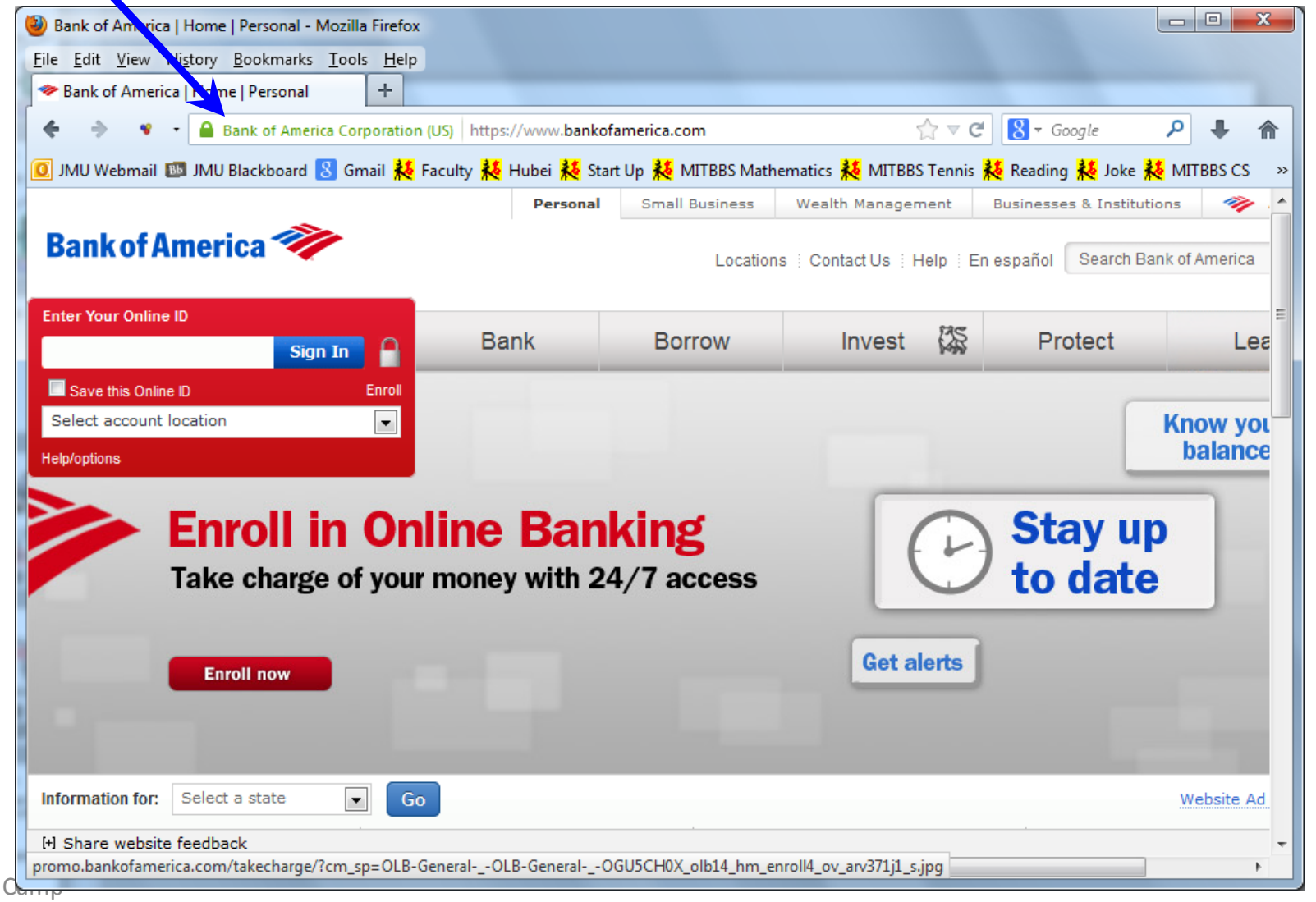
- Q: How is a key-pair like a hand grenade?
- A: You get two parts, there's no aiming, & it's hard to use safely

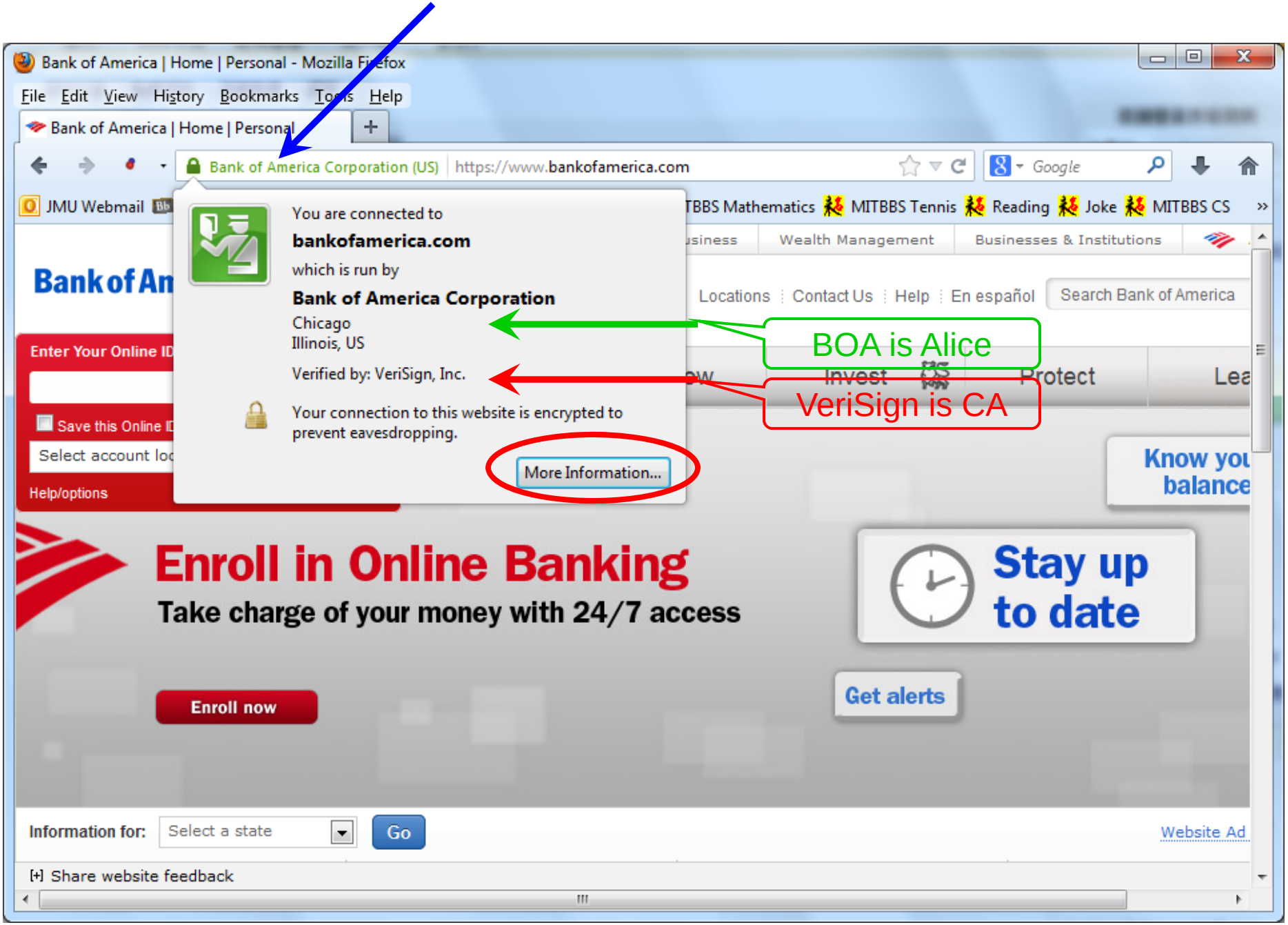
- Q: How are they different?
- A: With a grenade, you throw the dangerous part away …

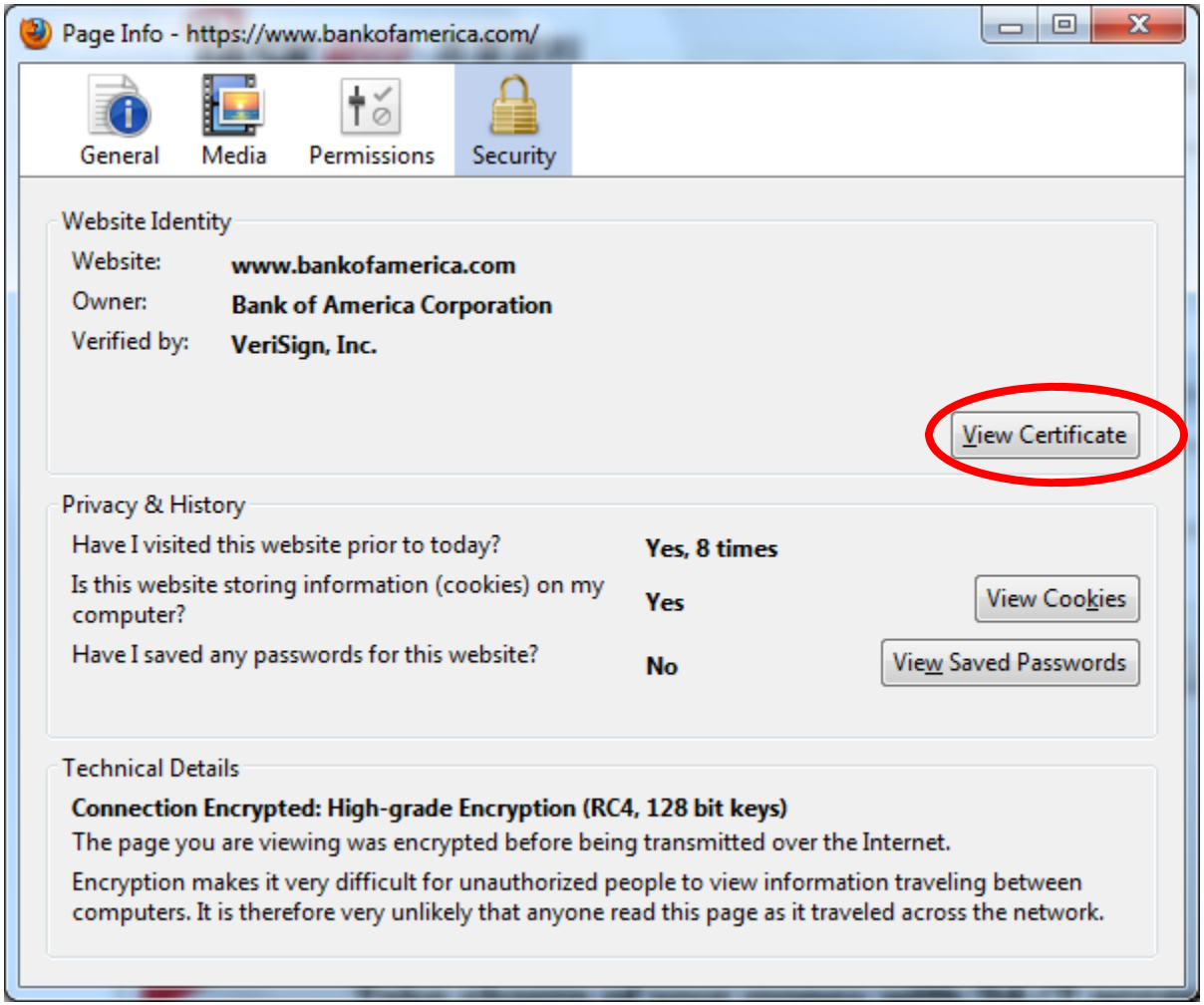
Road Map

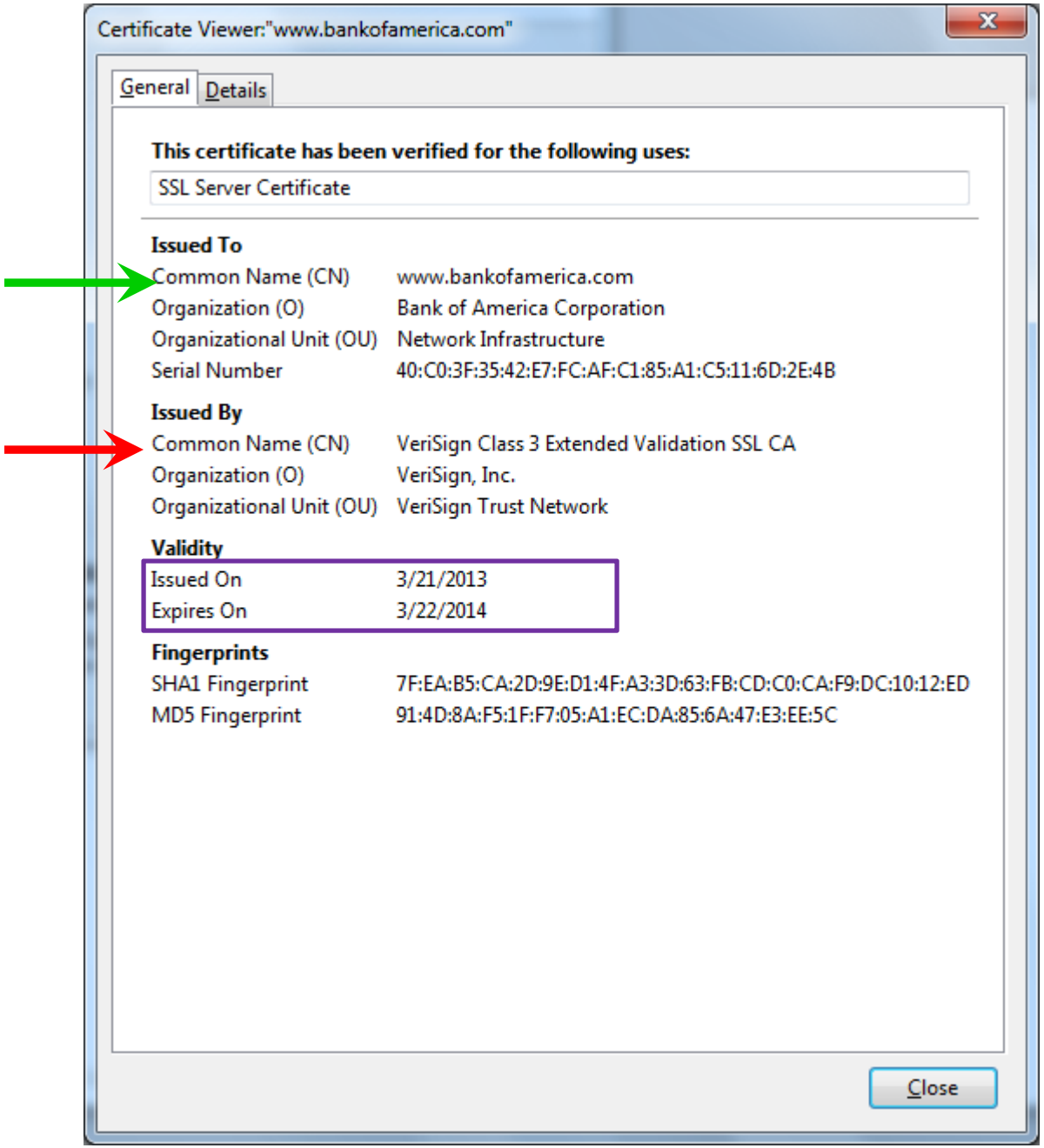
- The data confidentiality problem
- Theory
  - Numbers
  - Encryption
  - Digital signature
  - Cryptographic hashing
  - Digital certificates and PKI
- Tie everything together: HTTPS

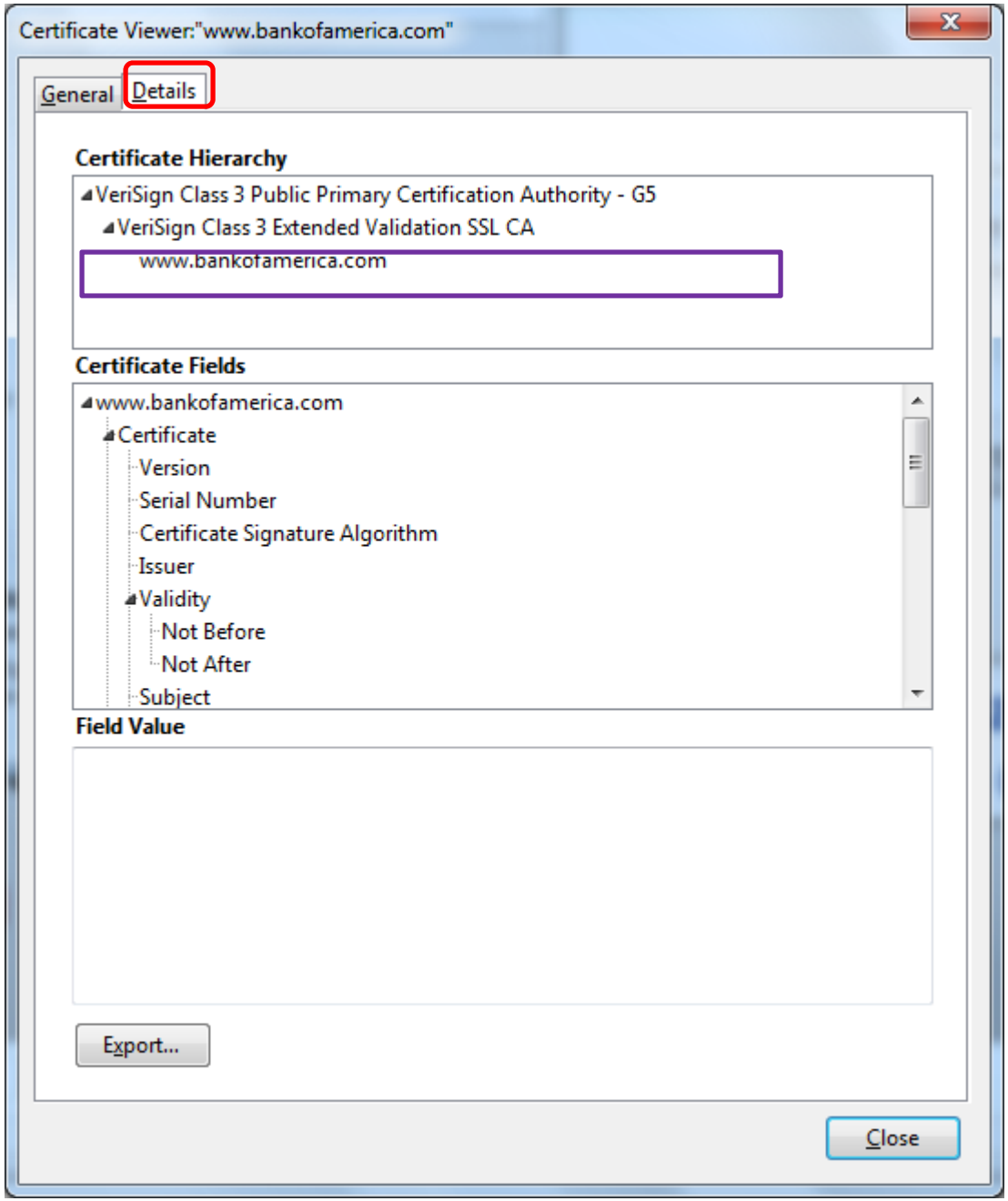
What is This?

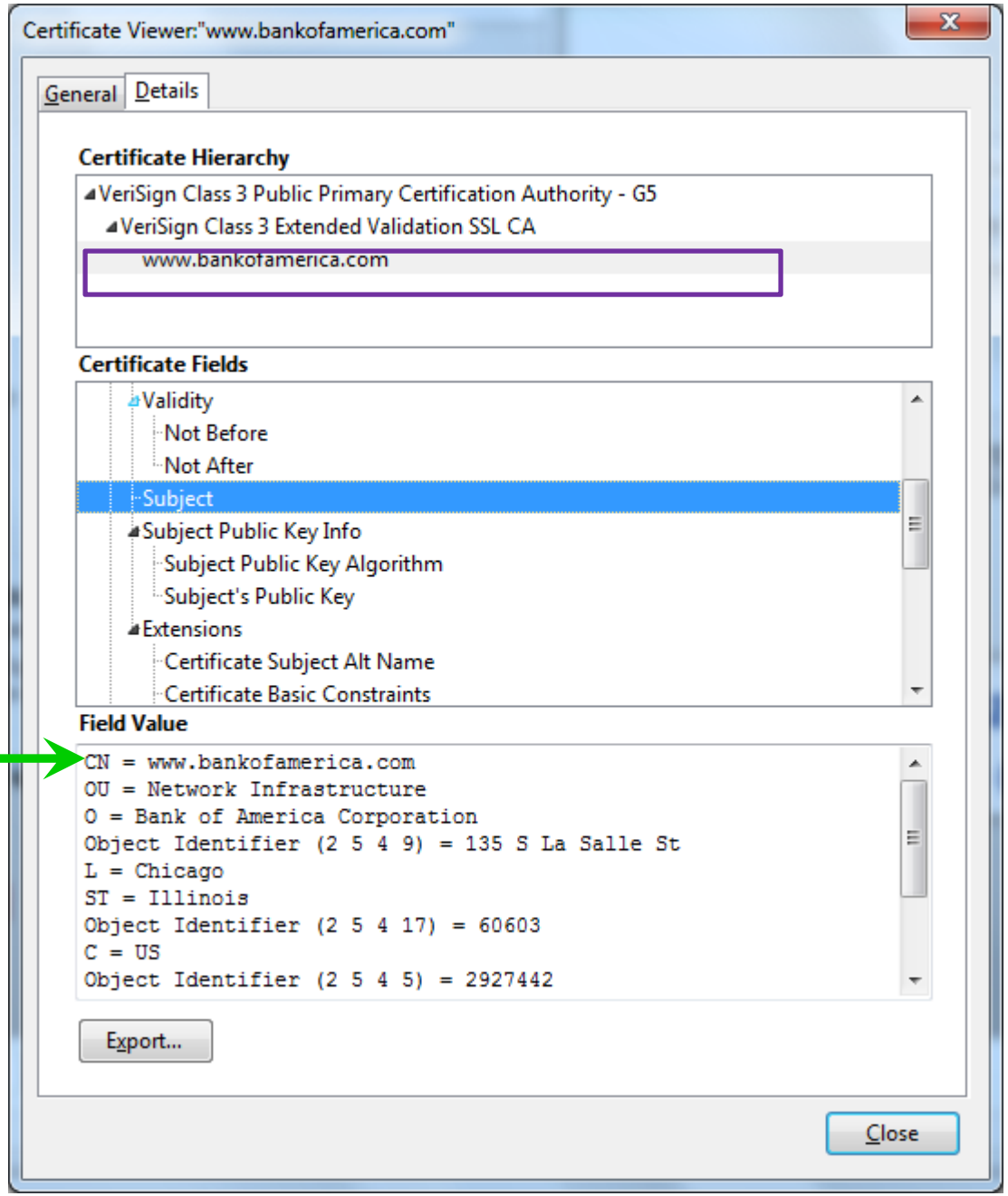

Bank of America | Home | Personal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Bank of America | Home | Personal
Bank of America Corporation (US) https://www.bankofamerica.com
Google
JMU Webmail JMU Blackboard Gmail Faculty Hubei Start Up MITBBS Mathematics MITBBS Tennis Reading Joke MITBBS CS
Personal Small Business Wealth Management Businesses & Institutions
Bank of America
Locations Contact Us Help En español Search Bank of America
Enter Your Online ID
Sign In
Save this Online ID Enroll
Select account location
Help/options
Bank Borrow Invest Protect
Know you balance
Enroll in Online Banking
Take charge of your money with 24/7 access
Stay up to date
Enroll now
Get alerts
Information for: Select a state Go
Website Ad
[+] Share website feedback
promo.bankofamerica.com/takecharge/?cm_sp=OLB-General-_-OLB-General-_-OGU5CH0X_olb14_hm_enroll4_ov_arv371j1_s.jpg

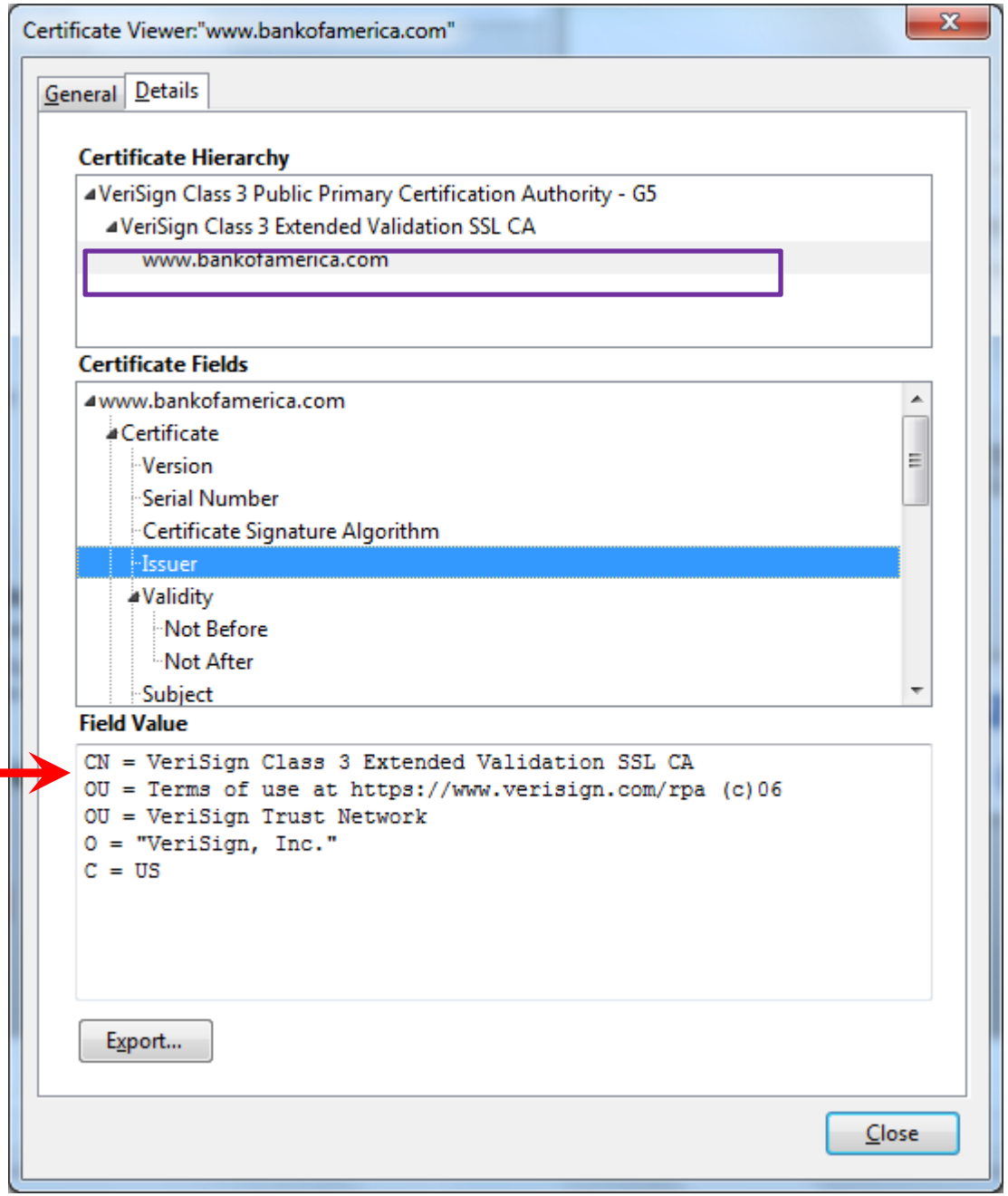

Bank of America | Home | Personal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Bank of America | Home | Personal
Bank of America Corporation (US)
https://www.bankofamerica.com
Google
JMU Webmail
MITBBS Mathematics
MITBBS Tennis
Reading
Joke
MITBBS CS
Wealth Management
Businesses & Institutions
Locations
Contact Us
Help
En español
Search Bank of America
Enter Your Online ID
Save this Online ID
Select account loc
Help/options
You are connected to
bankofamerica.com
which is run by
Bank of America Corporation
Chicago
Illinois, US
Verified by: VeriSign, Inc.
Your connection to this website is encrypted to prevent eavesdropping.
More Information...
BOA is Alice
VeriSign is CA
Invest
Protect
Know you balance
Enroll in Online Banking
Take charge of your money with 24/7 access
Enroll now
Stay up to date
Get alerts
Information for:
Select a state
Go
Website Ad
Share website feedback

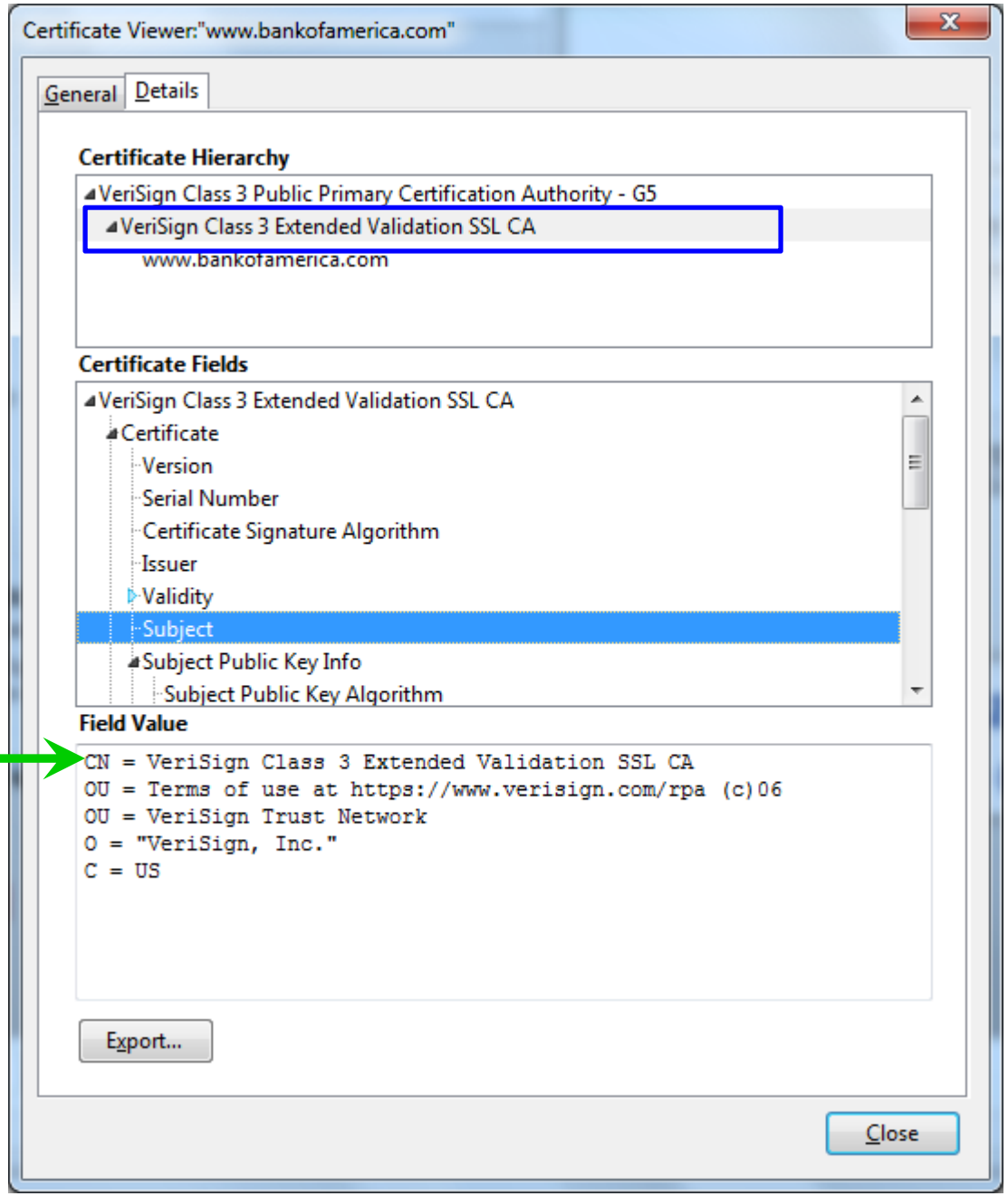

Page Info - https://www.bankofamerica.com/
General
Media
Permissions
Security
Website Identity
Website: www.bankofamerica.com
Owner: Bank of America Corporation
Verified by: VeriSign, Inc.
View Certificate
Privacy & History
Have I visited this website prior to today? Yes, 8 times
Is this website storing information (cookies) on my computer? Yes
View Cookies
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted: High-grade Encryption (RC4, 128 bit keys)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

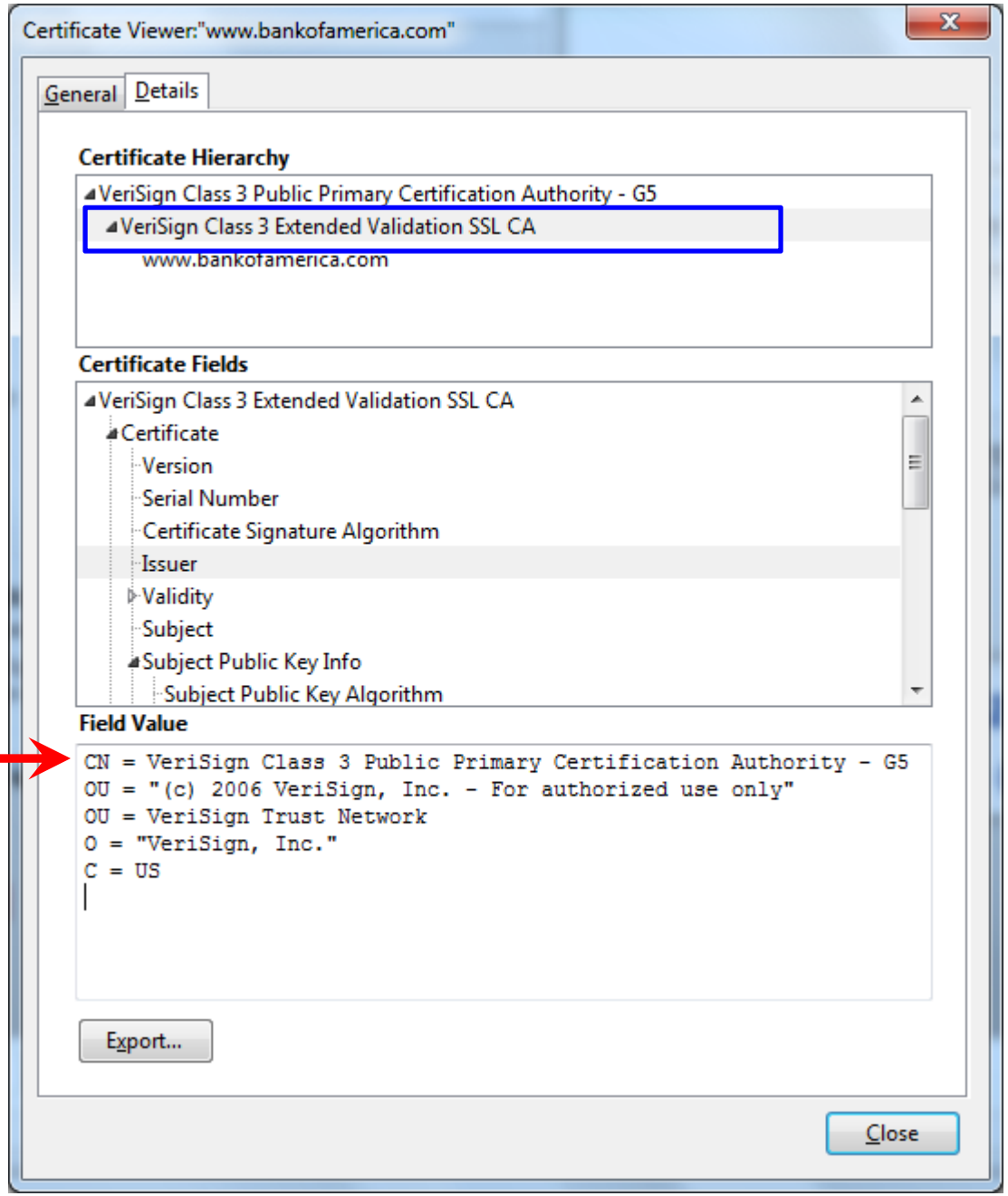

Certificate Viewer:"www.bankofamerica.com"
General
Details
This certificate has been verified for the following uses:
SSL Server Certificate
Issued To
Common Name (CN) www.bankofamerica.com
Organization (O) Bank of America Corporation
Organizational Unit (OU) Network Infrastructure
Serial Number 40:C0:3F:35:42:E7:FC:AF:C1:85:A1:C5:11:6D:2E:4B
Issued By
Common Name (CN) VeriSign Class 3 Extended Validation SSL CA
Organization (O) VeriSign, Inc.
Organizational Unit (OU) VeriSign Trust Network
Validity
Issued On 3/21/2013
Expires On 3/22/2014
Fingerprints
SHA1 Fingerprint 7F:EA:B5:CA:2D:9E:D1:4F:A3:3D:63:FB:CD:C0:CA:F9:DC:10:12:ED
MD5 Fingerprint 91:4D:8A:F5:1F:F7:05:A1:EC:DA:85:6A:47:E3:EE:5C
Close

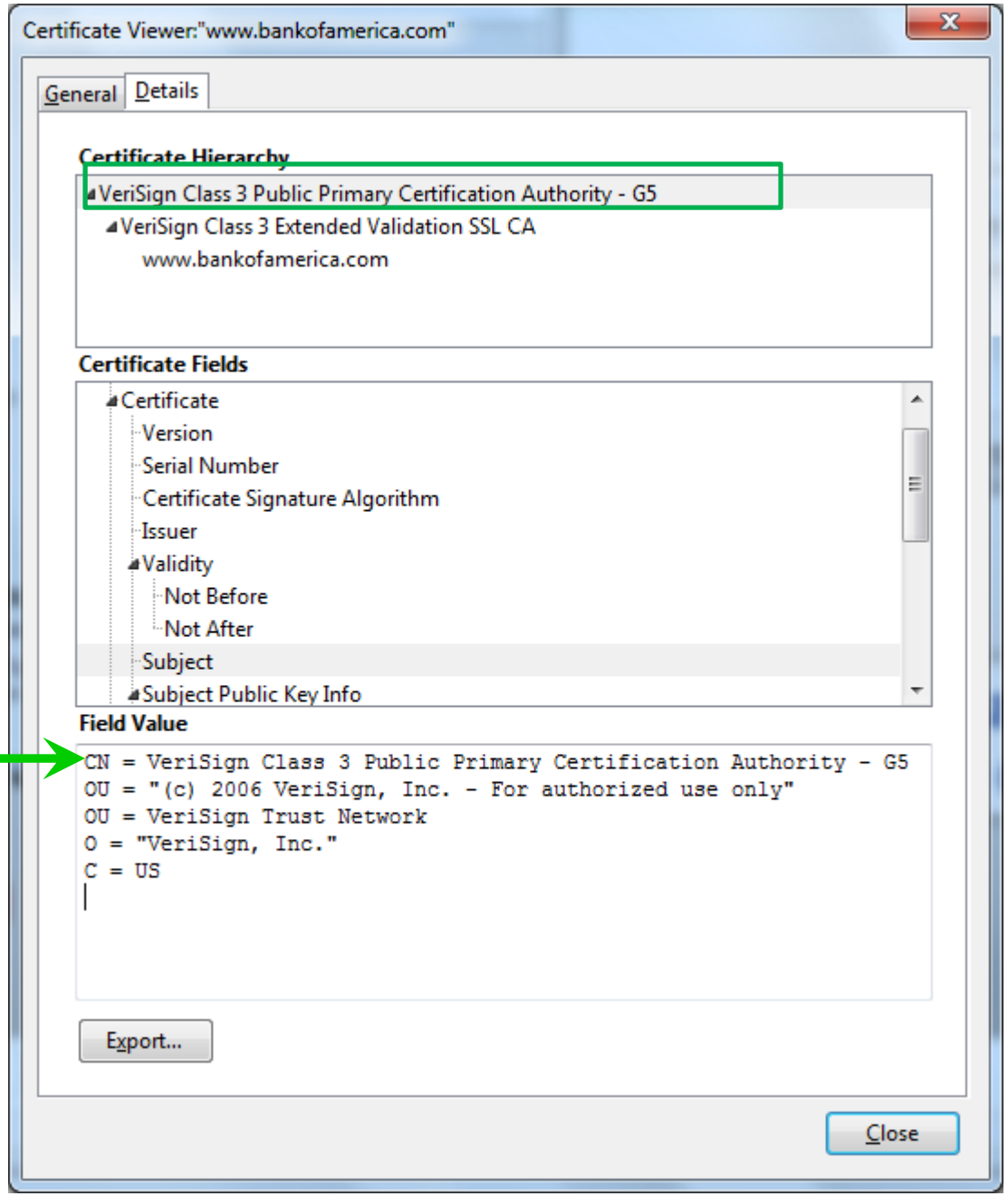

Certificate Viewer:"www.bankofamerica.com"
General
Details
Certificate Hierarchy
VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Extended Validation SSL CA
www.bankofamerica.com
Certificate Fields
www.bankofamerica.com
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Field Value
Export...
Close

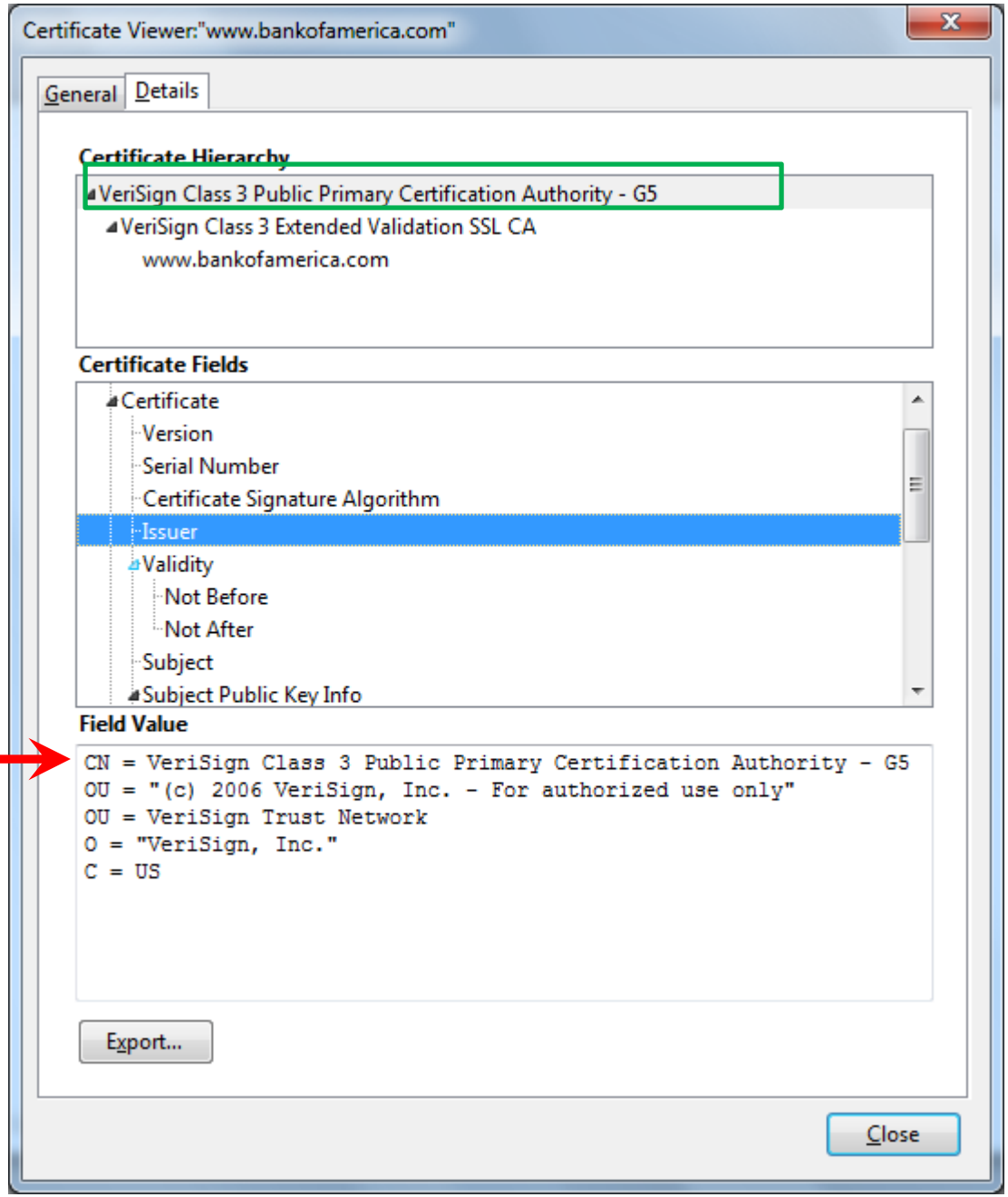

Certificate Viewer:"www.bankofamerica.com"
General
Details
Certificate Hierarchy
VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Extended Validation SSL CA
www.bankofamerica.com
Certificate Fields
Validity
Not Before
Not After
Subject
Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
Extensions
Certificate Subject Alt Name
Certificate Basic Constraints
Field Value
CN = www.bankofamerica.com
OU = Network Infrastructure
O = Bank of America Corporation
Object Identifier (2 5 4 9) = 135 S La Salle St
L = Chicago
ST = Illinois
Object Identifier (2 5 4 17) = 60603
C = US
Object Identifier (2 5 4 5) = 2927442
Export...
Close

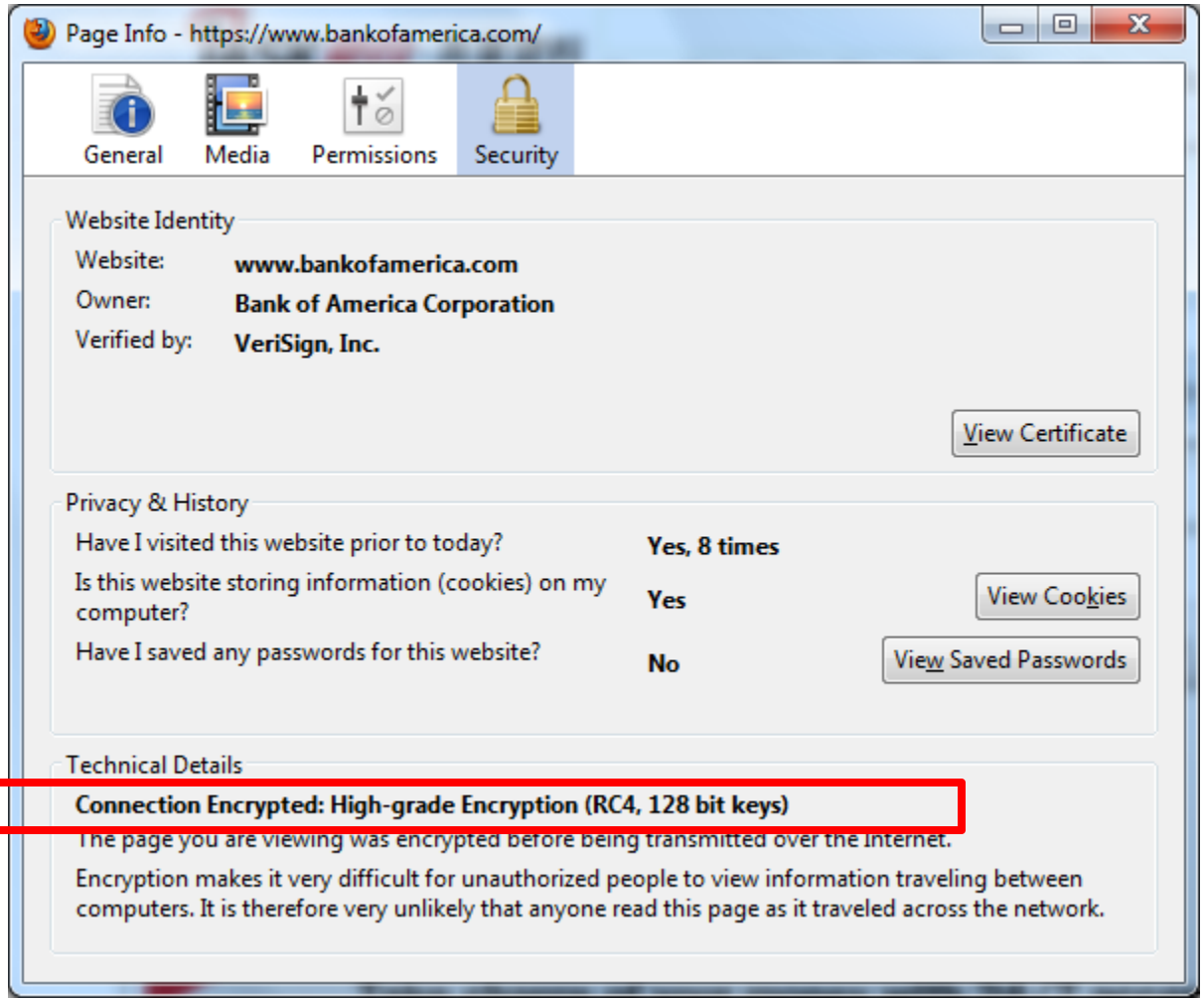

Certificate Viewer:"www.bankofamerica.com"
General
Details
Certificate Hierarchy
VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Extended Validation SSL CA
www.bankofamerica.com
Certificate Fields
www.bankofamerica.com
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Field Value
CN = VeriSign Class 3 Extended Validation SSL CA
OU = Terms of use at https://www.verisign.com/rpa (c)06
OU = VeriSign Trust Network
O = "VeriSign, Inc."
C = US
Export...
Close

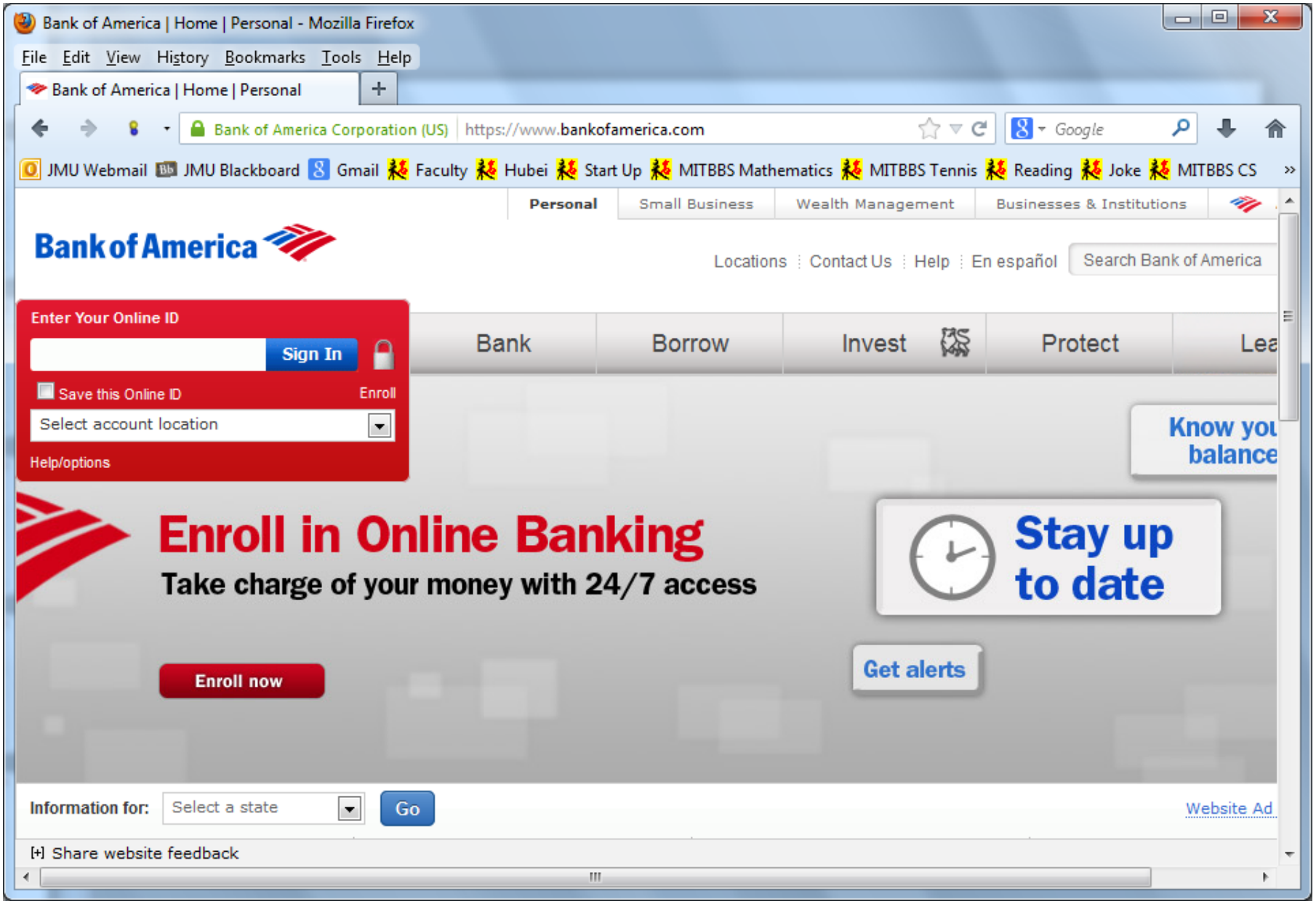

Certificate Viewer:"www.bankofamerica.com"
General
Details
Certificate Hierarchy
VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Extended Validation SSL CA
www.bankofamerica.com
Certificate Fields
VeriSign Class 3 Extended Validation SSL CA
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Subject
Subject Public Key Info
Subject Public Key Algorithm
Field Value
CN = VeriSign Class 3 Extended Validation SSL CA
OU = Terms of use at https://www.verisign.com/rpa (c)06
OU = VeriSign Trust Network
O = "VeriSign, Inc."
C = US
Export...
Close

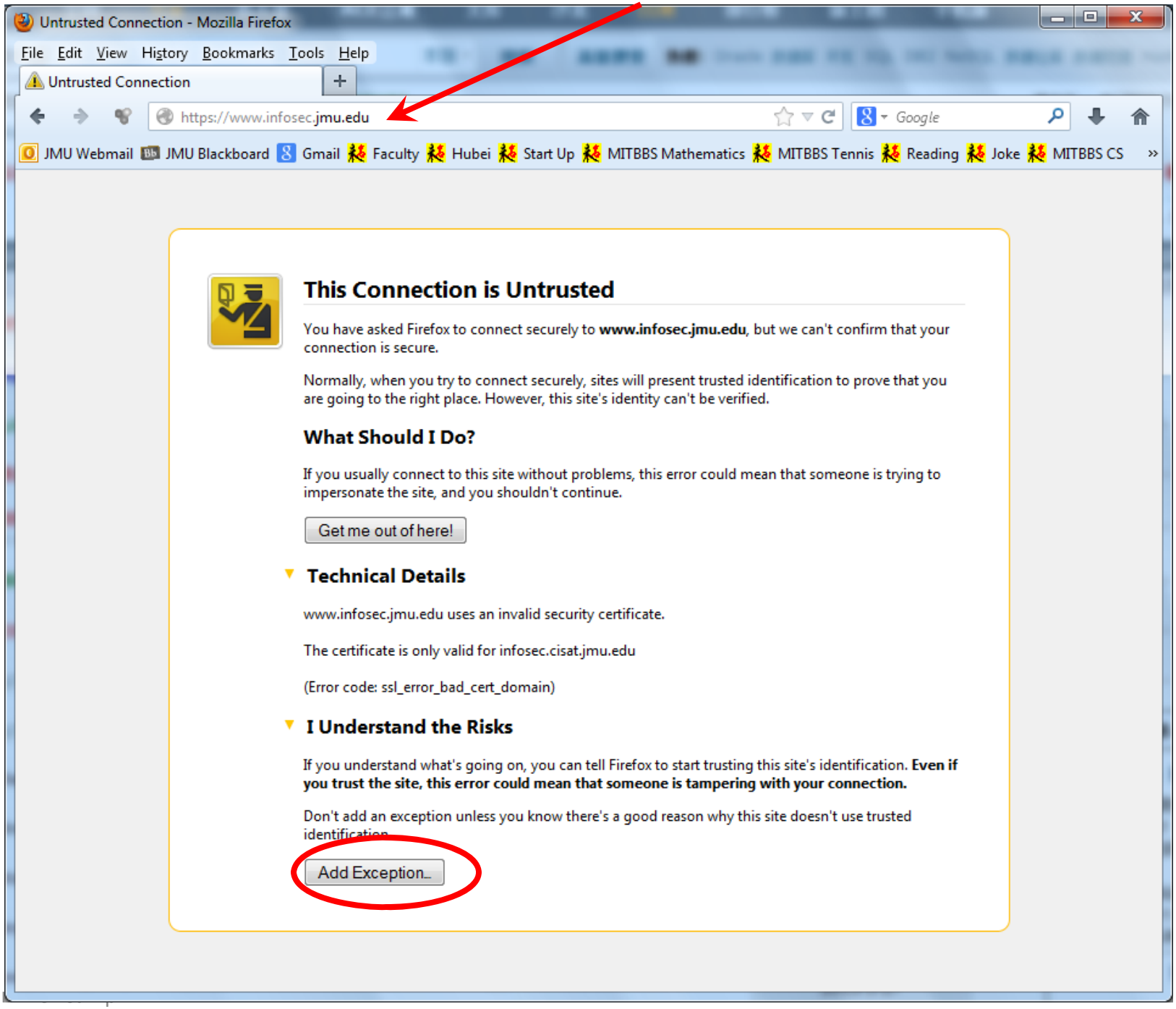

Certificate Viewer:"www.bankofamerica.com"
General
Details
Certificate Hierarchy
VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Extended Validation SSL CA
www.bankofamerica.com
Certificate Fields
VeriSign Class 3 Extended Validation SSL CA
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Subject
Subject Public Key Info
Subject Public Key Algorithm
Field Value
CN = VeriSign Class 3 Public Primary Certification Authority - G5
OU = "(c) 2006 VeriSign, Inc. - For authorized use only"
OU = VeriSign Trust Network
O = "VeriSign, Inc."
C = US
Export...
Close

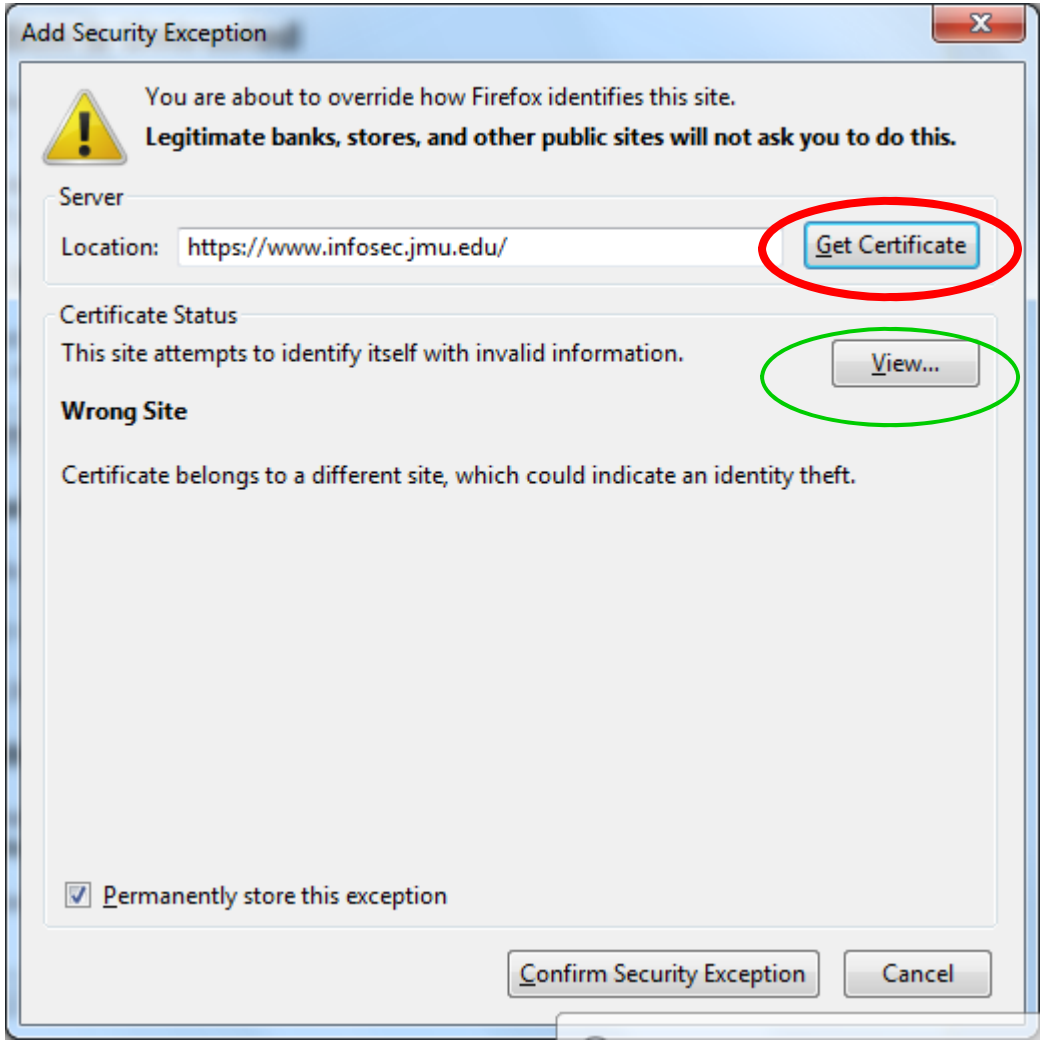

Certificate Viewer:"www.bankofamerica.com"
General
Details
Certificate Hierarchy
VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Extended Validation SSL CA
www.bankofamerica.com
Certificate Fields
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Subject Public Key Info
Field Value
CN = VeriSign Class 3 Public Primary Certification Authority - G5
OU = "(c) 2006 VeriSign, Inc. - For authorized use only"
OU = VeriSign Trust Network
O = "VeriSign, Inc."
C = US
Export...
Close

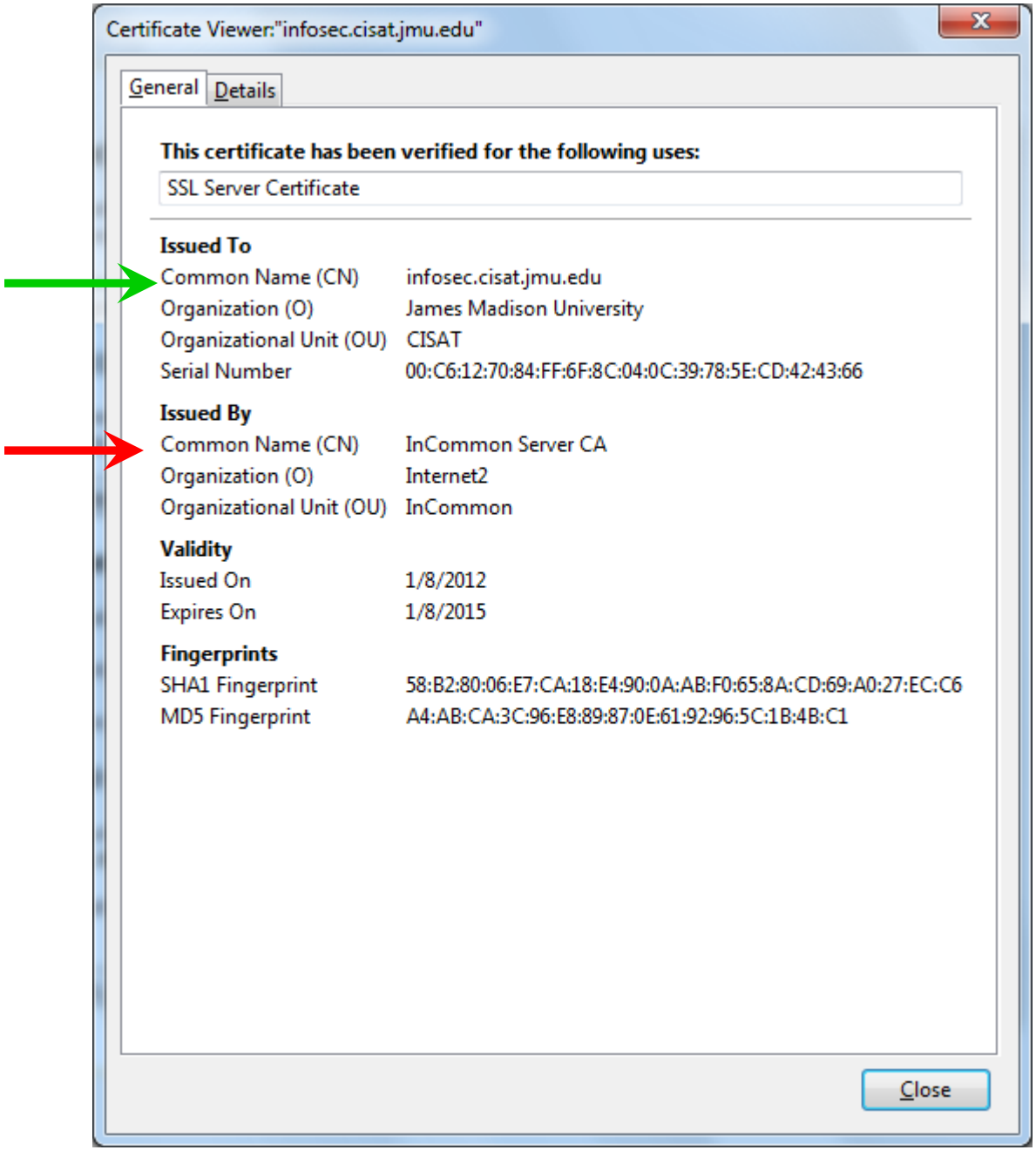

Certificate Viewer:"www.bankofamerica.com"
General
Details
Certificate Hierarchy
VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Extended Validation SSL CA
www.bankofamerica.com
Certificate Fields
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Subject Public Key Info
Field Value
CN = VeriSign Class 3 Public Primary Certification Authority - G5
OU = "(c) 2006 VeriSign, Inc. - For authorized use only"
OU = VeriSign Trust Network
O = "VeriSign, Inc."
C = US
Export...
Close

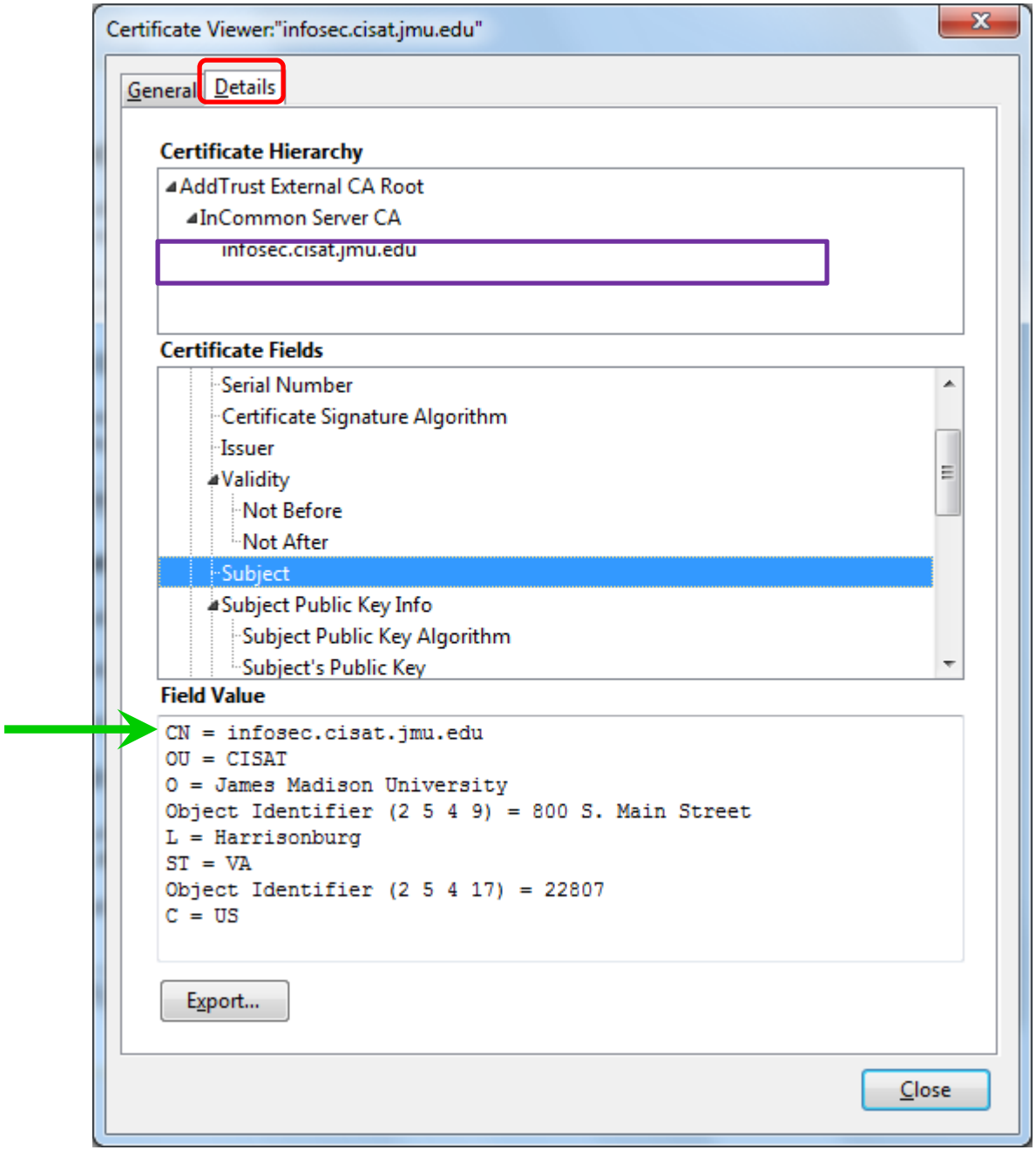

Page Info - https://www.bankofamerica.com/
General
Media
Permissions
Security
Website Identity
Website: www.bankofamerica.com
Owner: Bank of America Corporation
Verified by: VeriSign, Inc.
View Certificate
Privacy & History
Have I visited this website prior to today? Yes, 8 times
Is this website storing information (cookies) on my computer? Yes
View Cookies
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted: High-grade Encryption (RC4, 128 bit keys)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

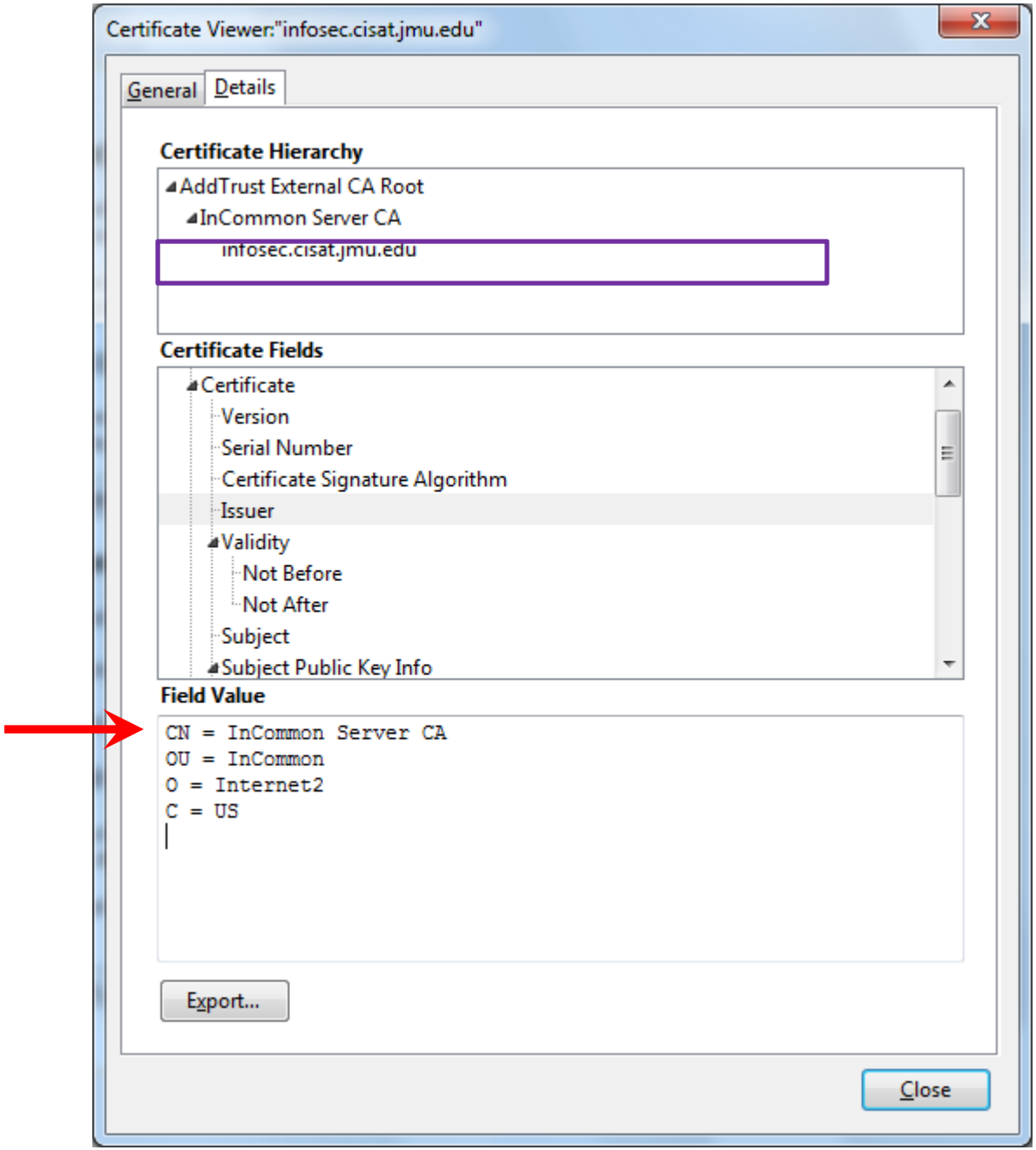

Bank of America | Home | Personal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Bank of America | Home | Personal
Bank of America Corporation (US) https://www.bankofamerica.com
Google
JMU Webmail JMU Blackboard Gmail Faculty Hubei Start Up MITBBS Mathematics MITBBS Tennis Reading Joke MITBBS CS
Personal Small Business Wealth Management Businesses & Institutions
Bank of America
Locations Contact Us Help En español Search Bank of America
Enter Your Online ID
Sign In
Save this Online ID
Enroll
Select account location
Help/options
Bank Borrow Invest Protect
Know you balance
Enroll in Online Banking
Take charge of your money with 24/7 access
Stay up to date
Enroll now
Get alerts
Information for:
Select a state
Go
Website Ad
[+] Share website feedback

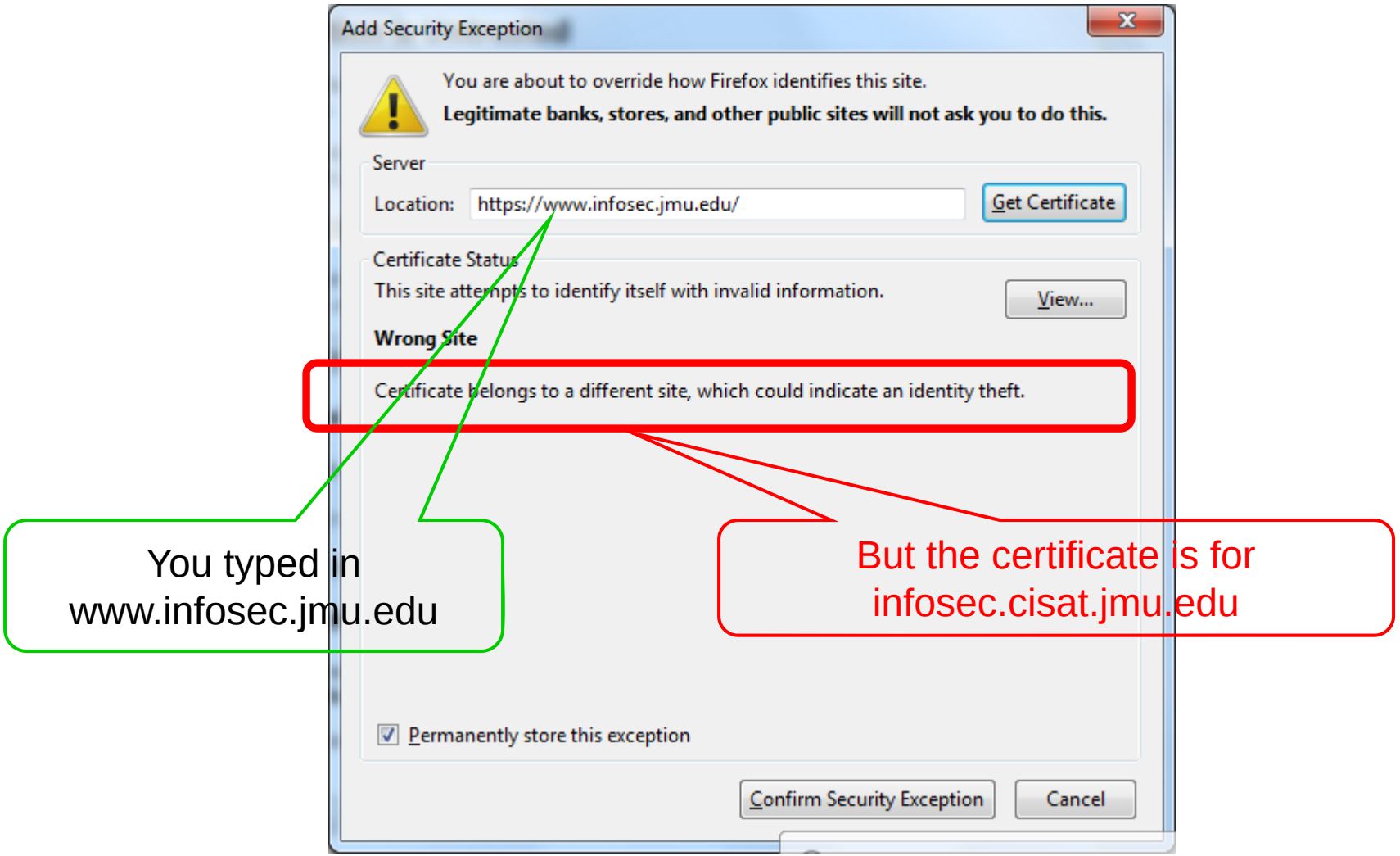

Untrusted Connection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Untrusted Connection
https://www.infosec.jmu.edu
Google
JMU Webmail JMU Blackboard Gmail Faculty Hubei Start Up MITBBS Mathematics MITBBS Tennis Reading Joke MITBBS CS
This Connection is Untrusted
You have asked Firefox to connect securely to www.infosec.jmu.edu, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
www.infosec.jmu.edu uses an invalid security certificate.
The certificate is only valid for infosec.cisat.jmu.edu
(Error code: ssl_error_bad_cert_domain)
I Understand the Risks
If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if you trust the site, this error could mean that someone is tampering with your connection.
Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.
Add Exception...


Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location: https://www.infosec.jmu.edu/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Permanently store this exception
Confirm Security Exception
Cancel


Certificate Viewer:"infosec.cisat.jmu.edu"
General
Details
This certificate has been verified for the following uses:
SSL Server Certificate
Issued To
Common Name (CN) infosec.cisat.jmu.edu
Organization (O) James Madison University
Organizational Unit (OU) CISAT
Serial Number 00:C6:12:70:84:FF:6F:8C:04:0C:39:78:5E:CD:42:43:66
Issued By
Common Name (CN) InCommon Server CA
Organization (O) Internet2
Organizational Unit (OU) InCommon
Validity
Issued On 1/8/2012
Expires On 1/8/2015
Fingerprints
SHA1 Fingerprint 58:B2:80:06:E7:CA:18:E4:90:0A:AB:F0:65:8A:CD:69:A0:27:EC:C6
MD5 Fingerprint A4:AB:CA:3C:96:E8:89:87:0E:61:92:96:5C:1B:4B:C1
Close


Certificate Viewer:"infosec.cisat.jmu.edu"
General
Details
Certificate Hierarchy
AddTrust External CA Root
InCommon Server CA
infosec.cisat.jmu.edu
Certificate Fields
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
Field Value
CN = infosec.cisat.jmu.edu
OU = CISAT
O = James Madison University
Object Identifier (2 5 4 9) = 800 S. Main Street
L = Harrisonburg
ST = VA
Object Identifier (2 5 4 17) = 22807
C = US
Export...
Close


Certificate Viewer:"infosec.cisat.jmu.edu"
General
Details
Certificate Hierarchy
AddTrust External CA Root
InCommon Server CA
infosec.cisat.jmu.edu
Certificate Fields
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Subject Public Key Info
Field Value
CN = InCommon Server CA
OU = InCommon
O = Internet2
C = US
Export...
Close


Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location: https://www.infosec.jmu.edu/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Permanently store this exception
Confirm Security Exception
Cancel
You typed in www.infosec.jmu.edu
But the certificate is for infosec.cisat.jmu.edu


Master's Degree in Information Security at JMU - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Master's Degree in Information Security ...
https://www.infosec.jmu.edu
Google
JMU Webmail JMU Blackboard Gmail Faculty Hubei Start Up MITBBS Mathematics MITBBS Tennis Reading Joke MITBBS CS
JAMES MADISON UNIVERSITY
DEPARTMENT OF COMPUTER SC
Master's Degree in
OMPUTER SCIENCE
CONCENTRATION IN INFORMATION SECURITY
Support Us | Find Us | Contac
SEARCH:
Home
About
Curriculum
Our People
Student Resources
Resear
Announcements
Clubs and Organizations
May 3 - 4
Commencement
One of the Original Seven National Centers of Academic Excellence in Information Assurance Education 4011, 4012, 4013, 4014, and 4015 Certified
Welcome to the InfoSe Program
The online education Information Security (Ir Master's pr at James M University to the need working professionals. The on program is delivered to student asynchronously over the Interr courses are available anytime any location. More >
News
See All
JMU InfoSec Joins CyberWatch
January 2012
JMU is one the new members of the CyberWatch. CyberWatch is an Advanced Technological Education (ATE) Center, headquartered at Prince George's Community College and funded by a grant from the National Science Foundation (NSF).
iNFOSE
Information Security Master's Pr
JAMES MADISON UNIVER

Summary

- The data confidentiality problem
- Theory
  - Numbers
  - Encryption
  - Digital signature
  - Cryptographic hashing
  - Digital certificates and PKI
- Tie everything together: HTTPS