



# Cryptography: Basics & Applications

2015 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?

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

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?

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

$$\text{In } 2^x?$$

$$\leq 2^{17}$$

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

- 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?

$$31,536,000 \text{ seconds} = 3.1536 \times 10^9$$

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





# 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:  $30 \text{ days} \times 86,400 = 2,592,000$  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
- $3.45 \times 10^9 \text{ Hz}$
- Clock rate:  $3.45 \times 10^9$  times per second
- Assumption:  $3.45 \times 10^9$  basic operations per second
  - ❖  $3.45 \times 10^9 < 2^{32}$ ;
- So in 100 years, this CPU can exhaust  $2^{32} \times 2^{32} = 2^{64}$  basic operations



# Nov. 2014

- Fastest computer:
  - <http://www.top500.org/>
- Tianhe-2
  - ❖ 33.86 petaflop/s (quadrillions of calculations per second) on the Linpack benchmark
  - ❖  $33.86 \times 10^{15} \approx 10^{16.53} \approx 2^{55}$  **calculations** per second
- 100 years  $\approx 2^{32}$  seconds
- 100 year's calculations:  $2^{55} \times 2^{32} = 2^{87}$



# What if 1000000 Such Supercomputers?

- One supercomputer:  $33.86 \times 10^{15} \approx 10^{16.53}$
- 1000000 ( $10^6$ ) such computers
  - ✦  $10^{22.53}$  calculations per second
  - $\approx 2^{74.85}$
- 100 years:  $2^{32}$  seconds
- 100 years' calculations = ?  
 $2^{74.85} \times 2^{32} \leq 2^{107}$



# What if 1 **billion** Such Supercomputers?

- One supercomputer:  $33.86 \times 10^{15} \approx 10^{16.53} \approx 2^{55}$  calculations per second
- **10000000000** ( $10^9 \approx 2^{29.9}$ ) such computers  
 $2^{55} \times 2^{29.9} \approx 2^{85}$  calculations per second
- 100 years:  $2^{32}$  seconds
- How many calculations in 100 years?  
 $2^{85} \times 2^{32} \approx 2^{117}$

**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?  $2^{87}$
- **1 million** fastest computers in 100 years:  $2^{107}$
- **1 billion** fastest computers in 100 years:  $2^{117}$



# 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)  
 $\approx 2^{57}$

Three-letter agency 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  $62^8 = 218340105584896$  ( **$\approx 2^{48}$** )
  - $\{\text{'!@#$%^&*()~',,./:~<>?|{}[]\}\} = 90$ , thus the total combinations are at most  $127^8$   
 **$\approx 2^{56}$**

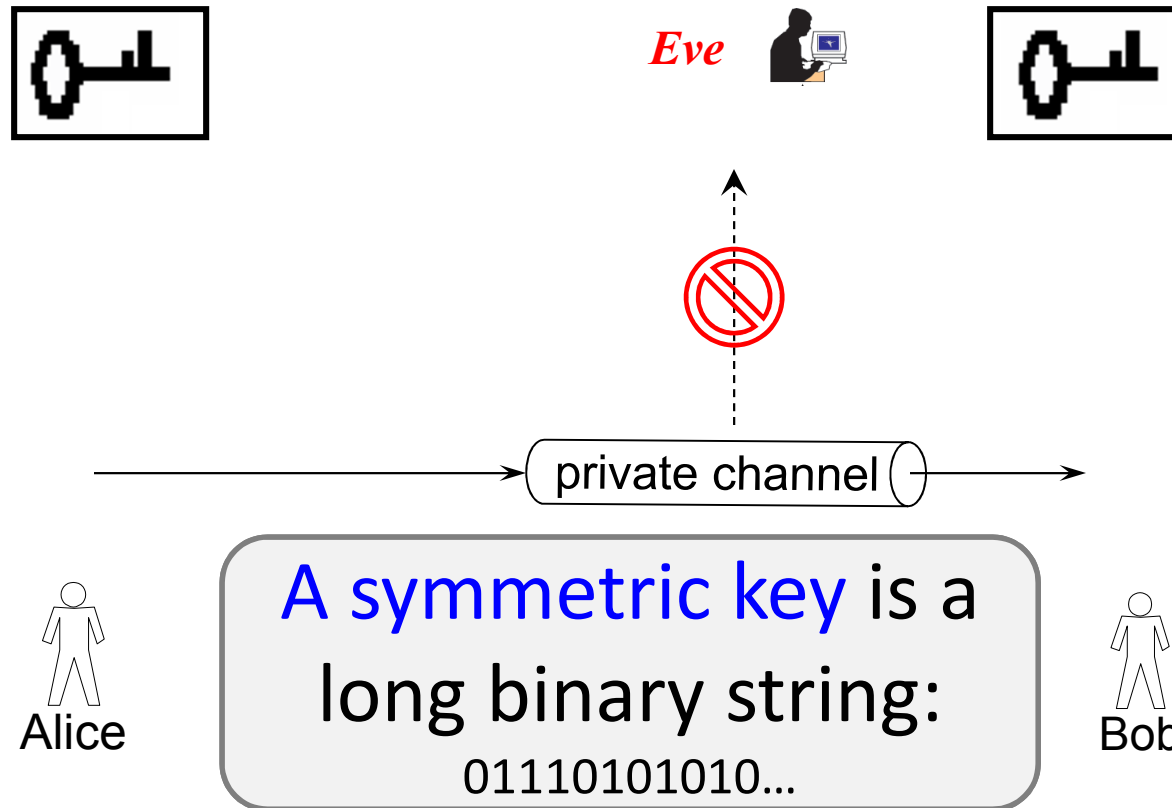
Roughly 4 seconds for the fastest computer



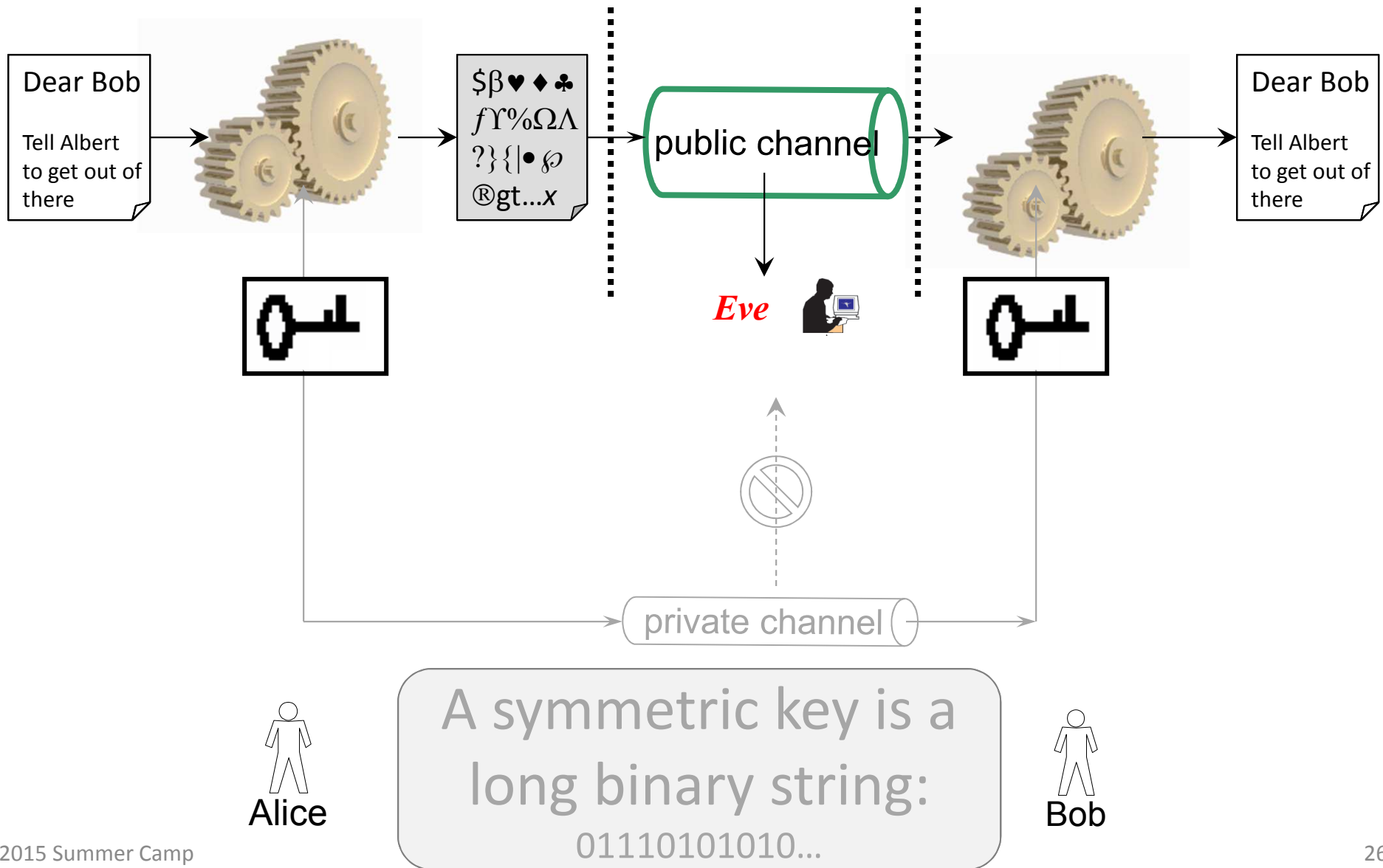
# Road Map

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

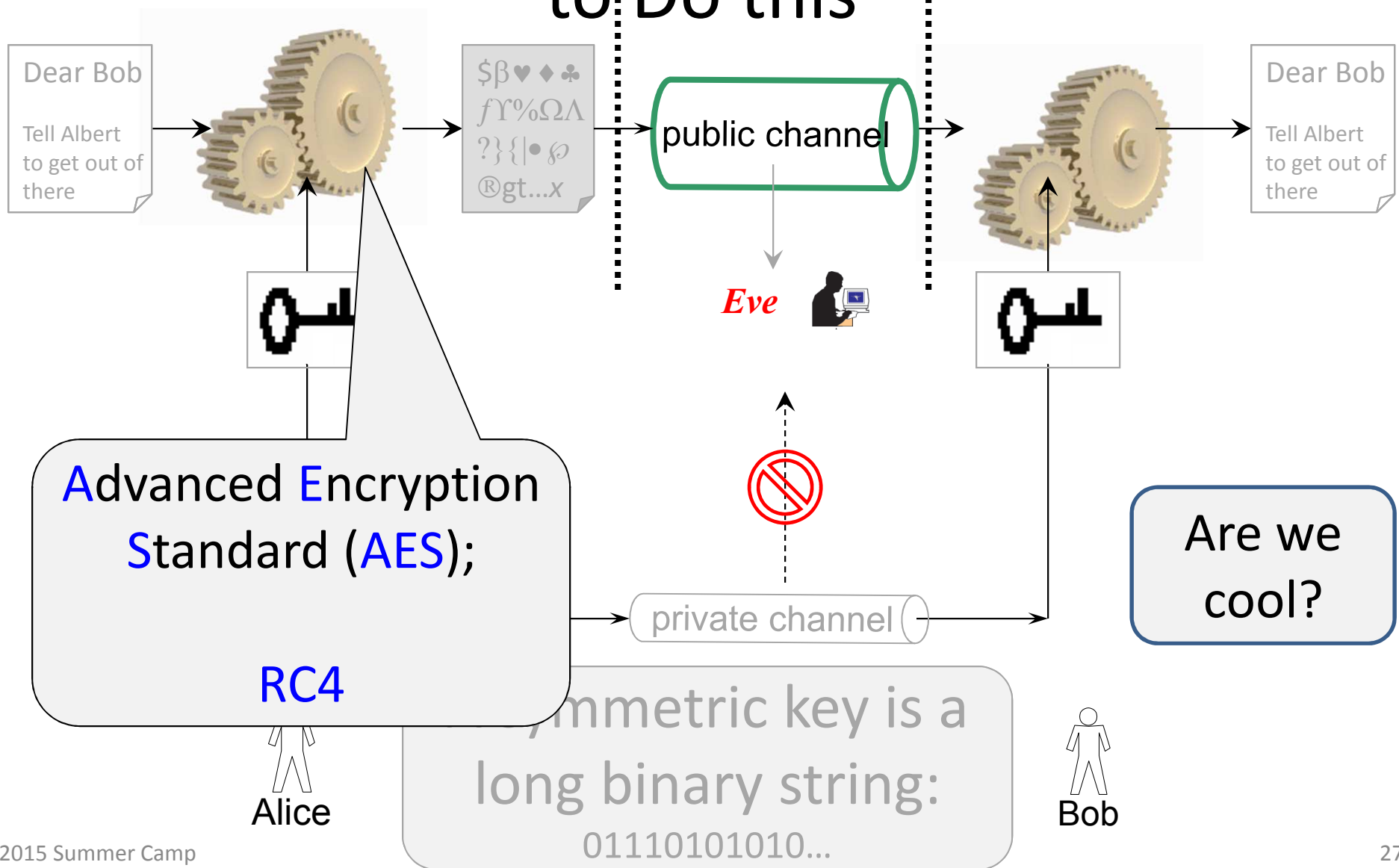
# Symmetric Key Encryption



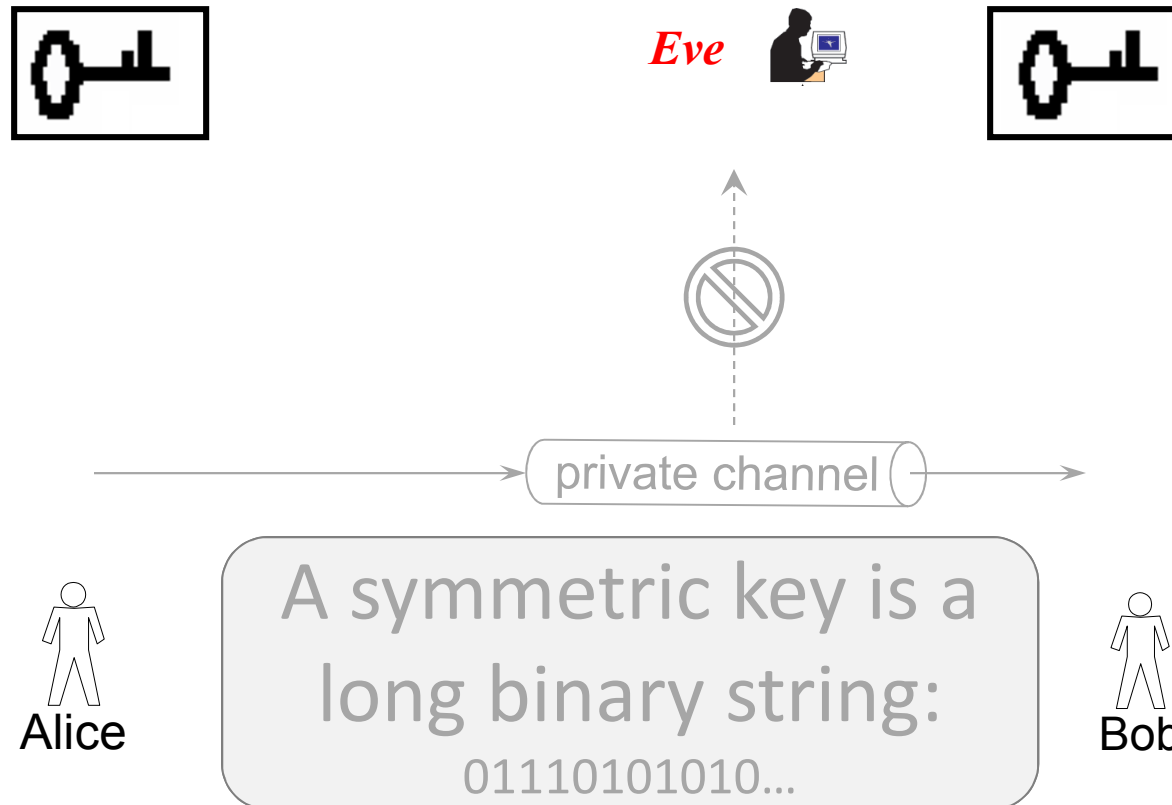
# Symmetric Key Encryption



# After 2000 years, We “Know” How to Do this

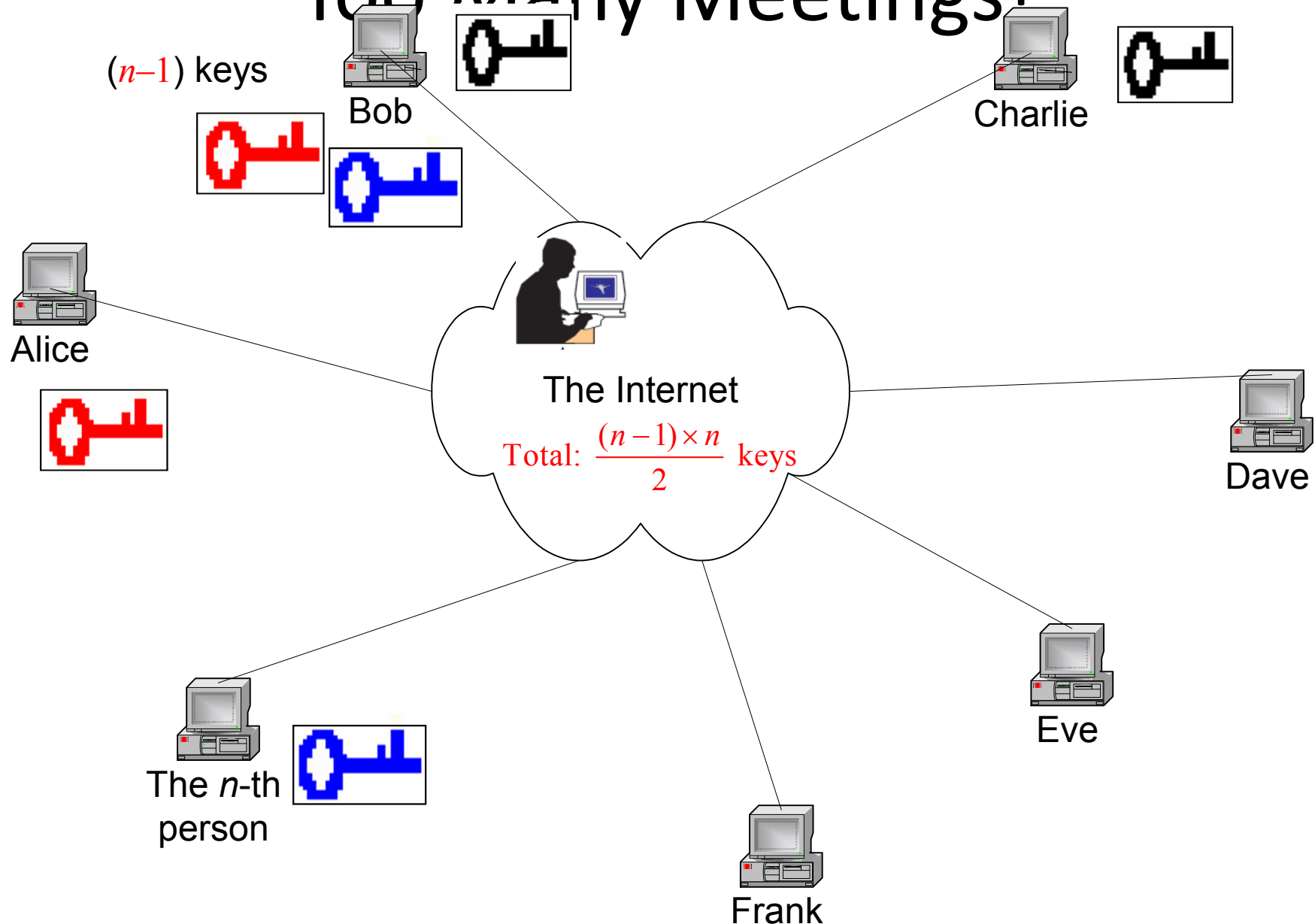


# Personal Meetings?



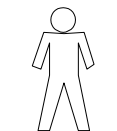


# Too Many Meetings!



# What if ...

Eve is able to monitor **all** communications between Alice and Bob (**all** the time)



Alice

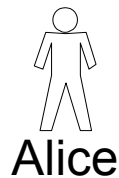
Can Alice still send Bob a  
**SECRET** message?



Bob

# What if ...

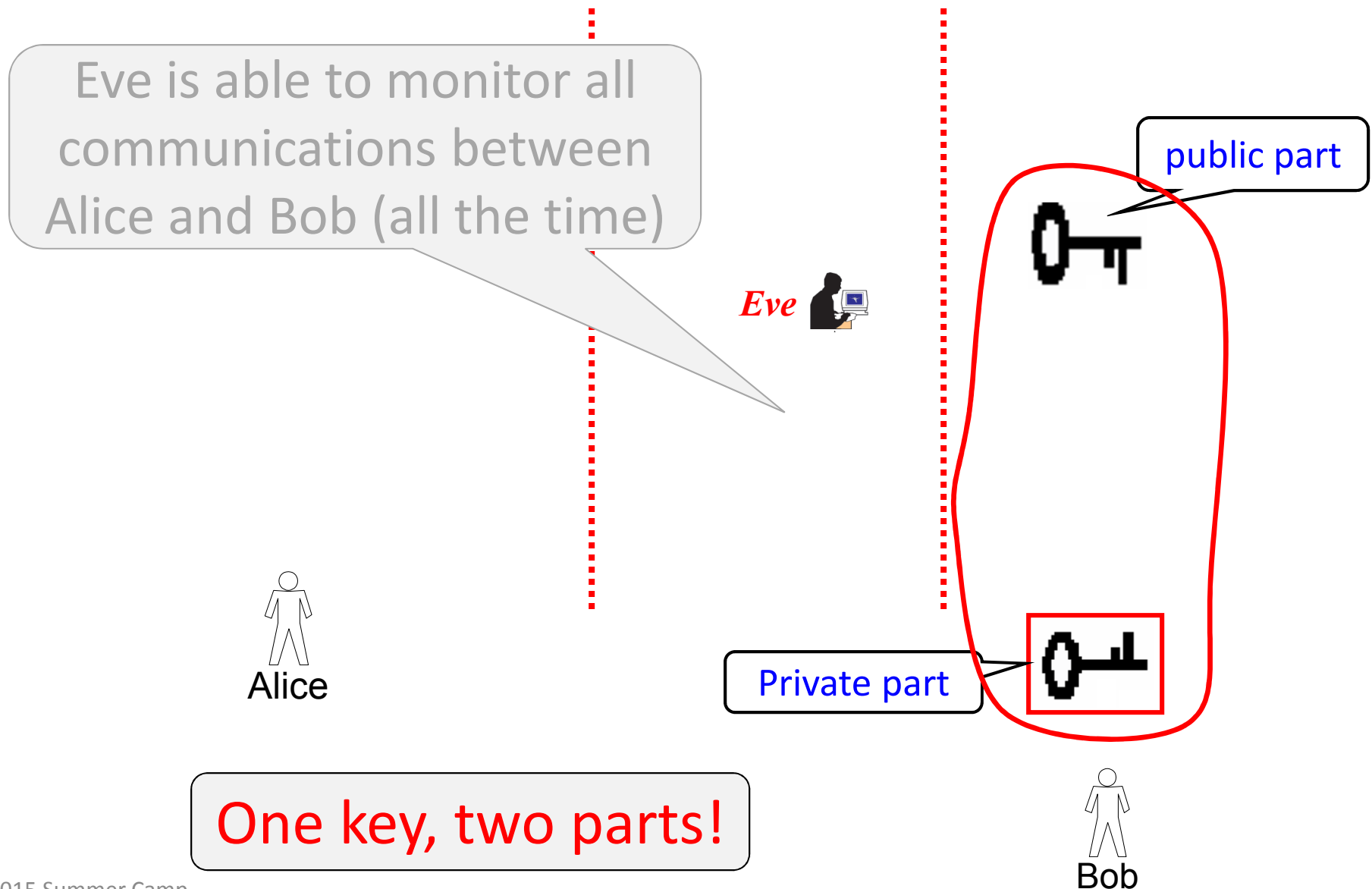
Eve is able to monitor all communications between Alice and Bob (all the time)



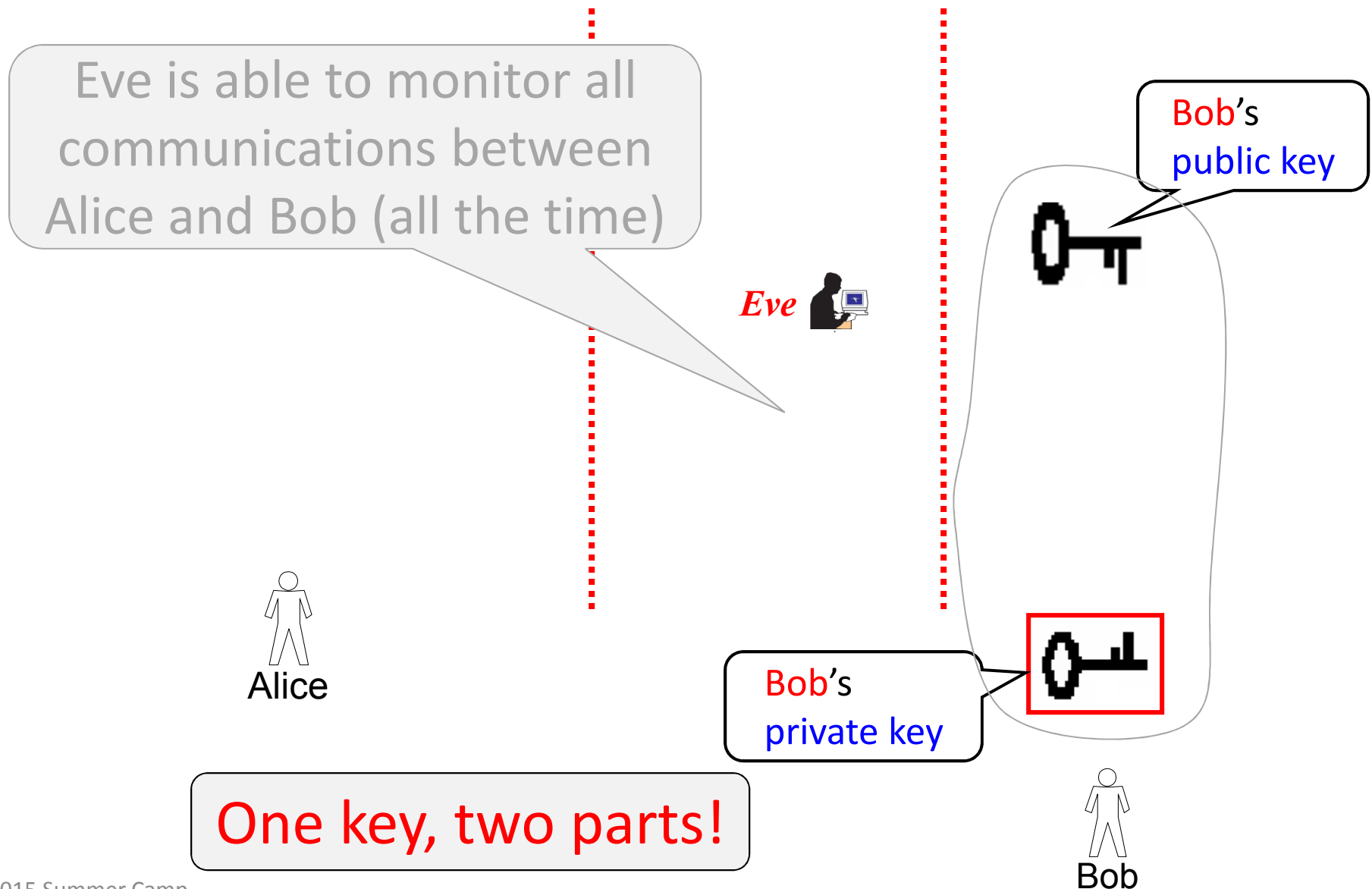
Can Alice still send Bob a secret message?



# What if ...



# What if ...

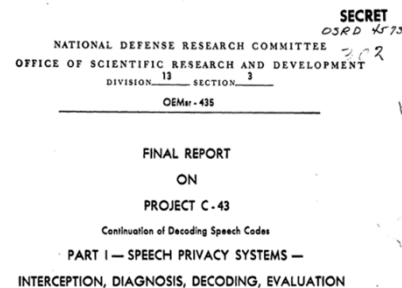


# How Did They Get Here?

- Two independent discoveries: 1969; 1975



Project C-43 (1944):  
involve the receiver



Password  
authentication

IFF

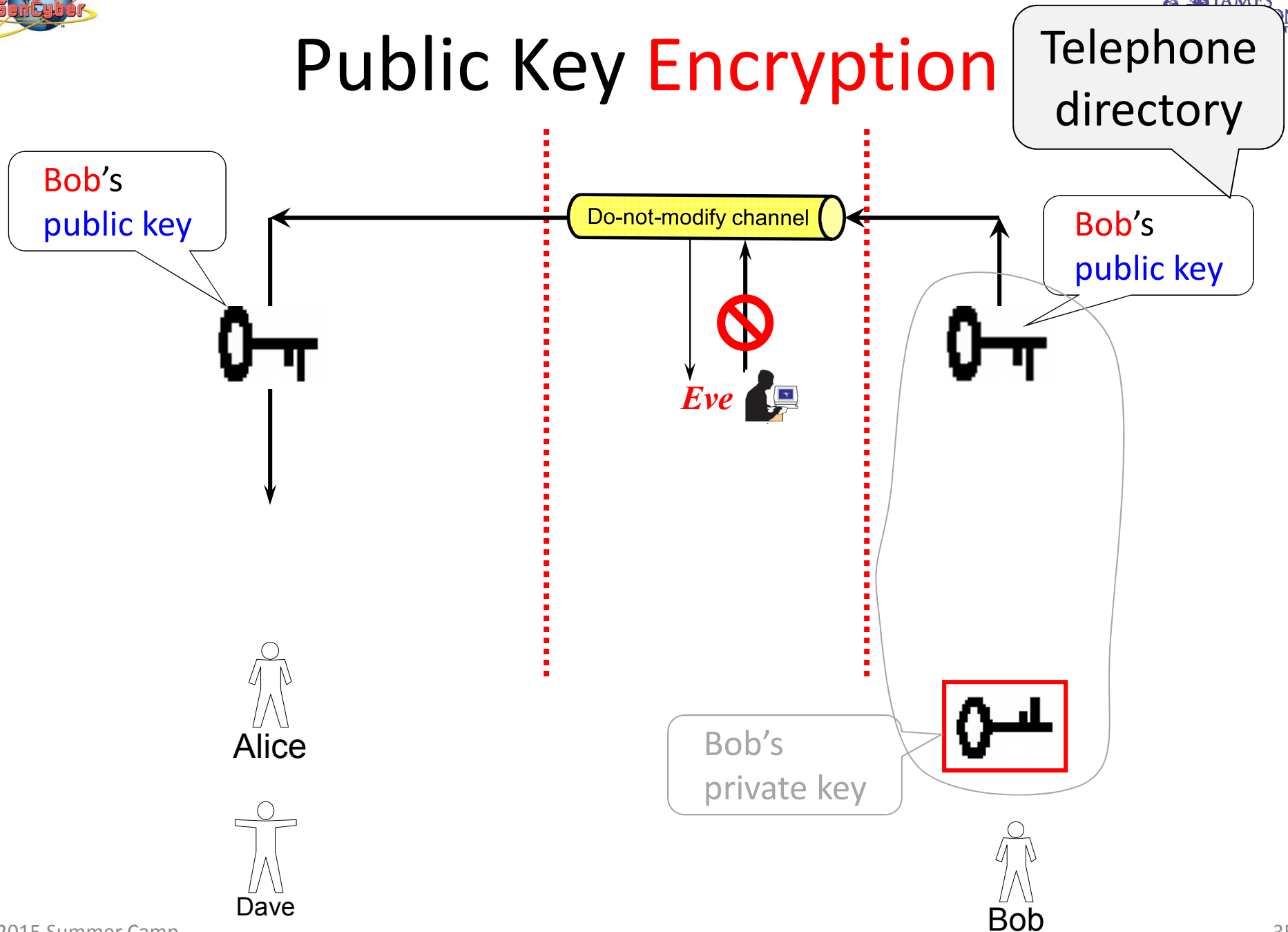
One-way function

One-way trapdoor  
function

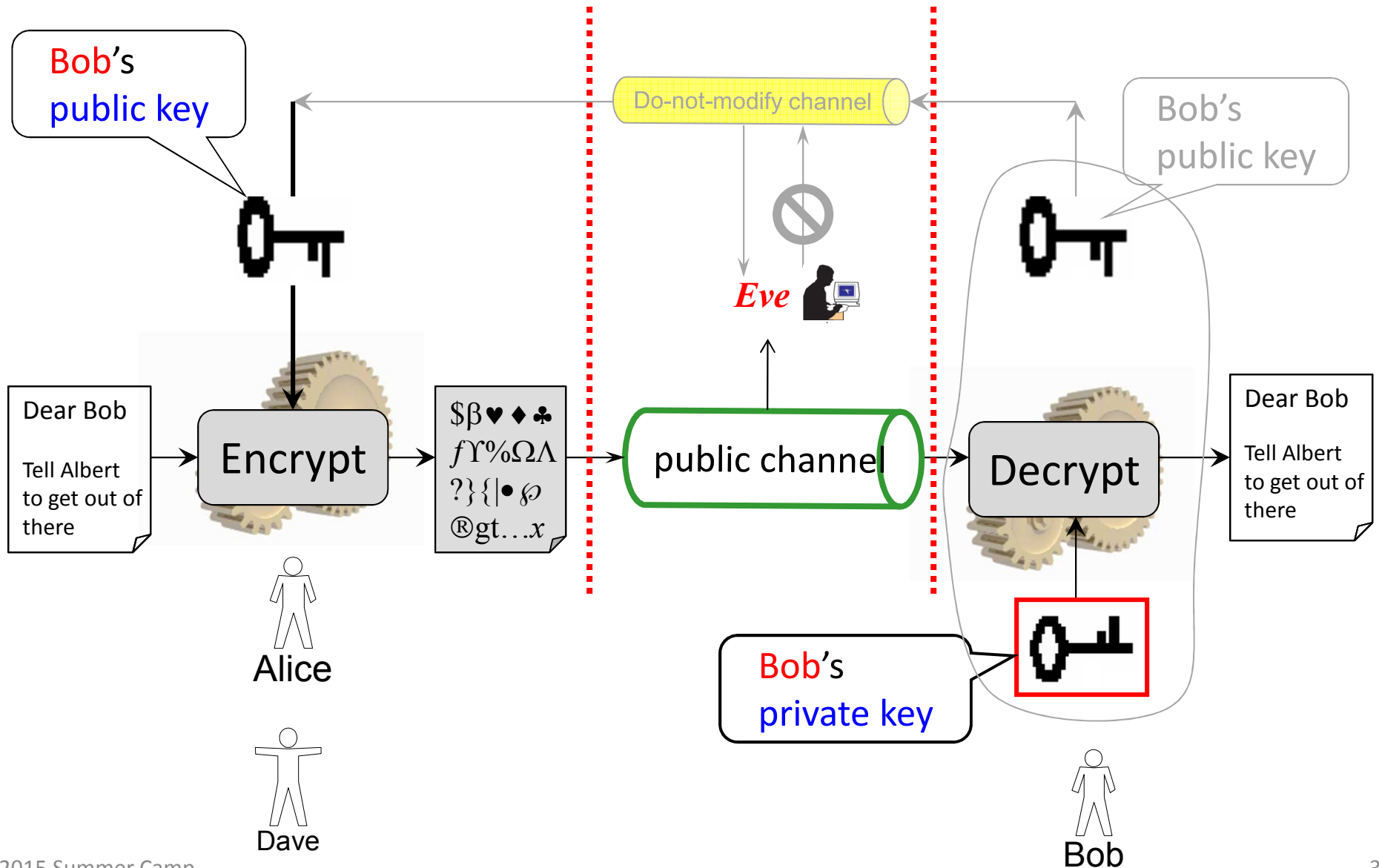




# Public Key Encryption

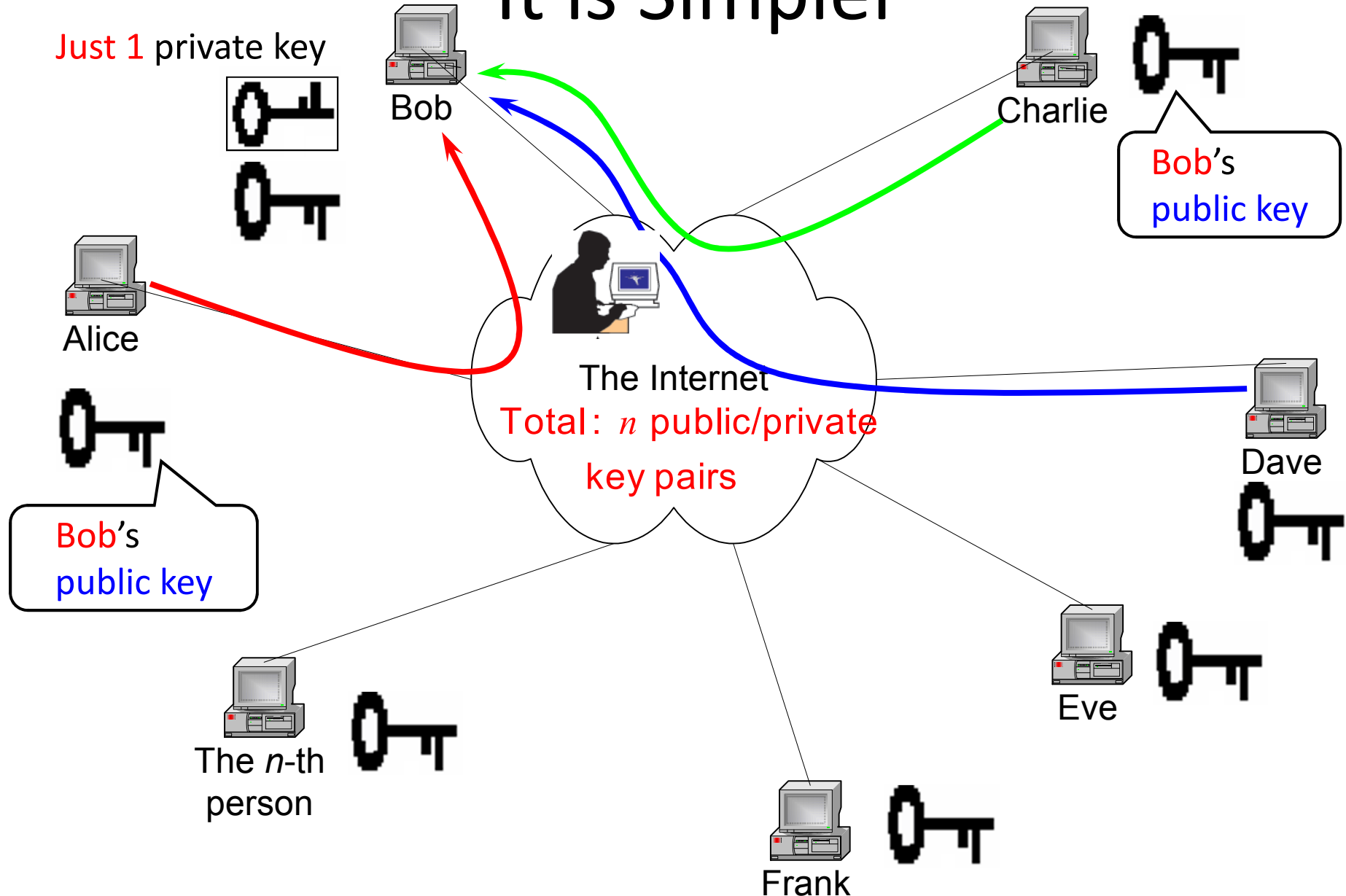


# Public Key Encryption





# It is Simpler





# Crypto 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?

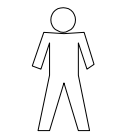
- Eat in a restaurant?
  - Sign your credit card payment
- Rent a house?
  - Sign the contract
- Get a car loan?
  - Sign the contract

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

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

# What if ...

Eve is able to monitor all communications between Alice and Bob (all the time)



Alice

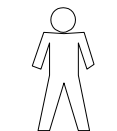
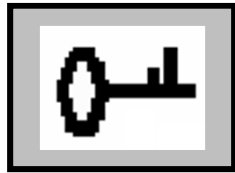
Can Alice digitally sign a message?



Bob

# Again, No Private Channels ...

Eve is able to monitor all communications between Alice and Bob (all the time)



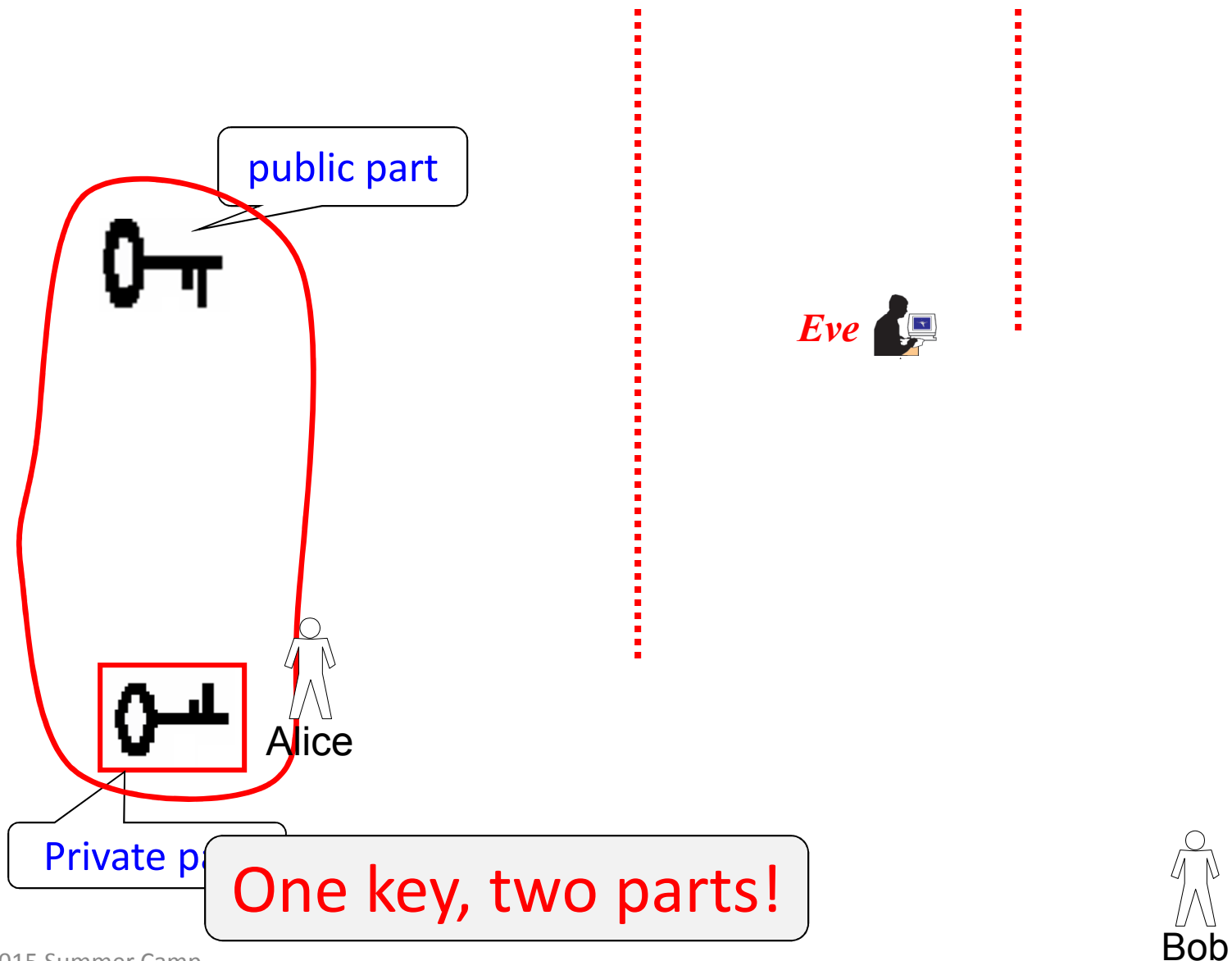
Alice

Can Alice digitally sign a message?

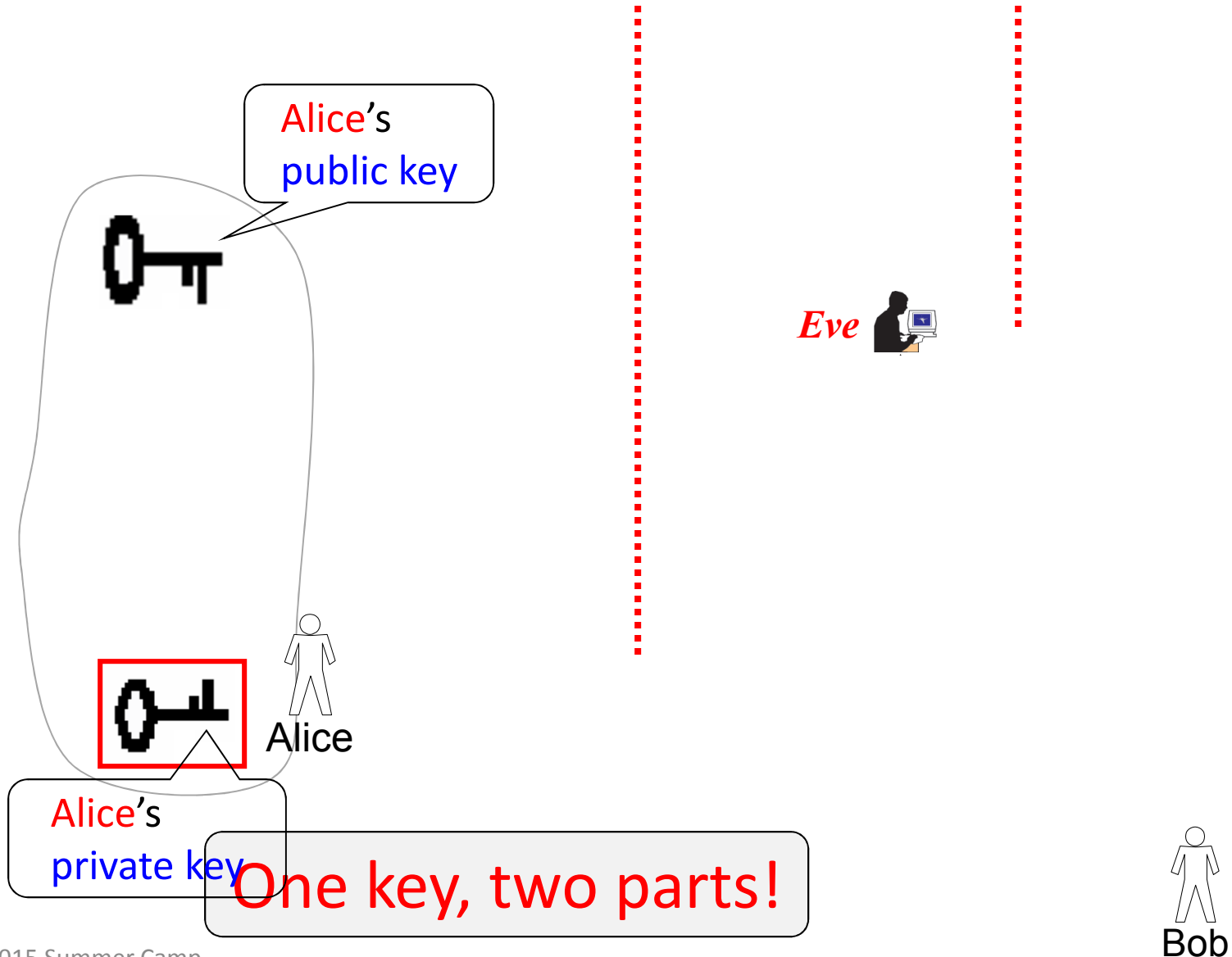


Bob

# Again, No Private Channels ...

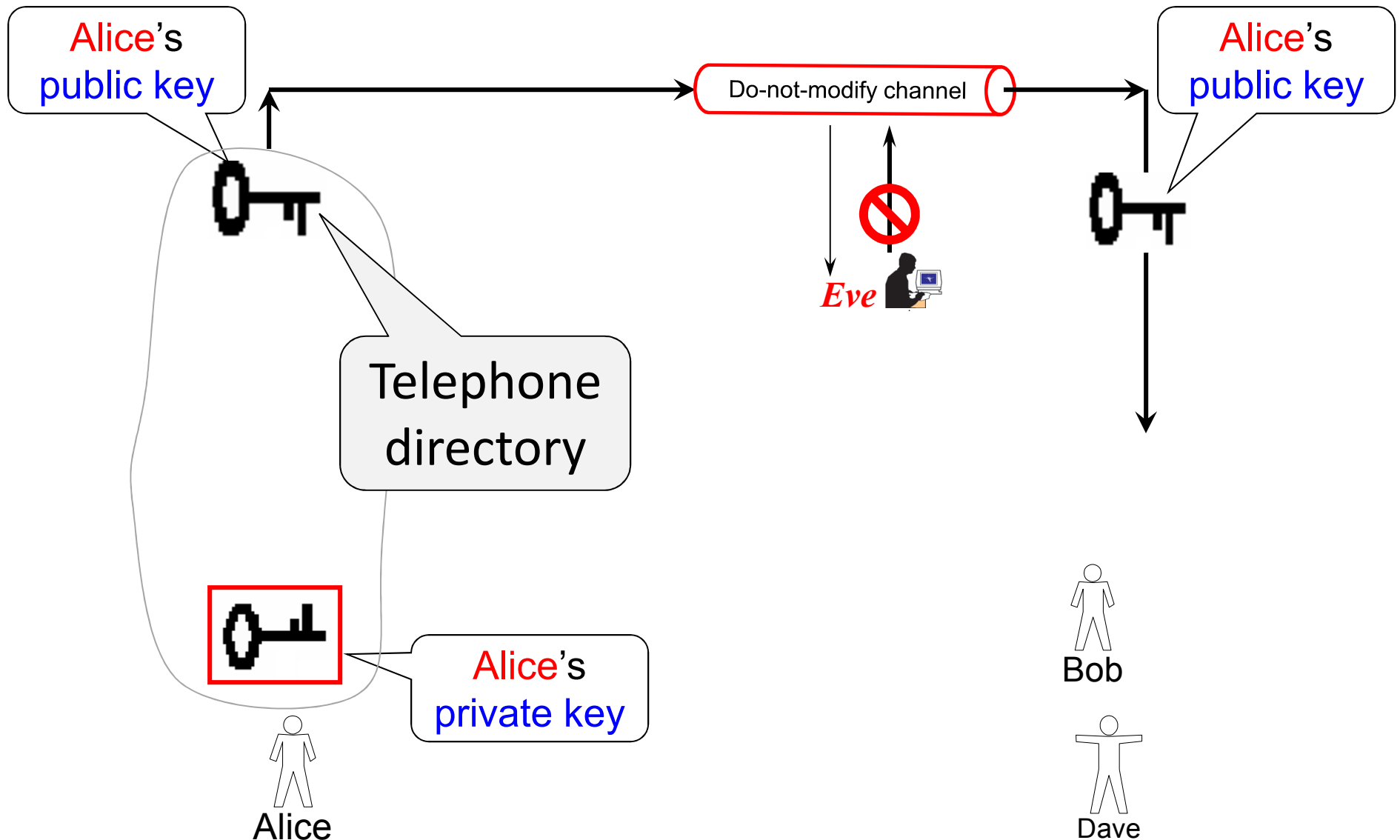


# Public-key Digital Signature

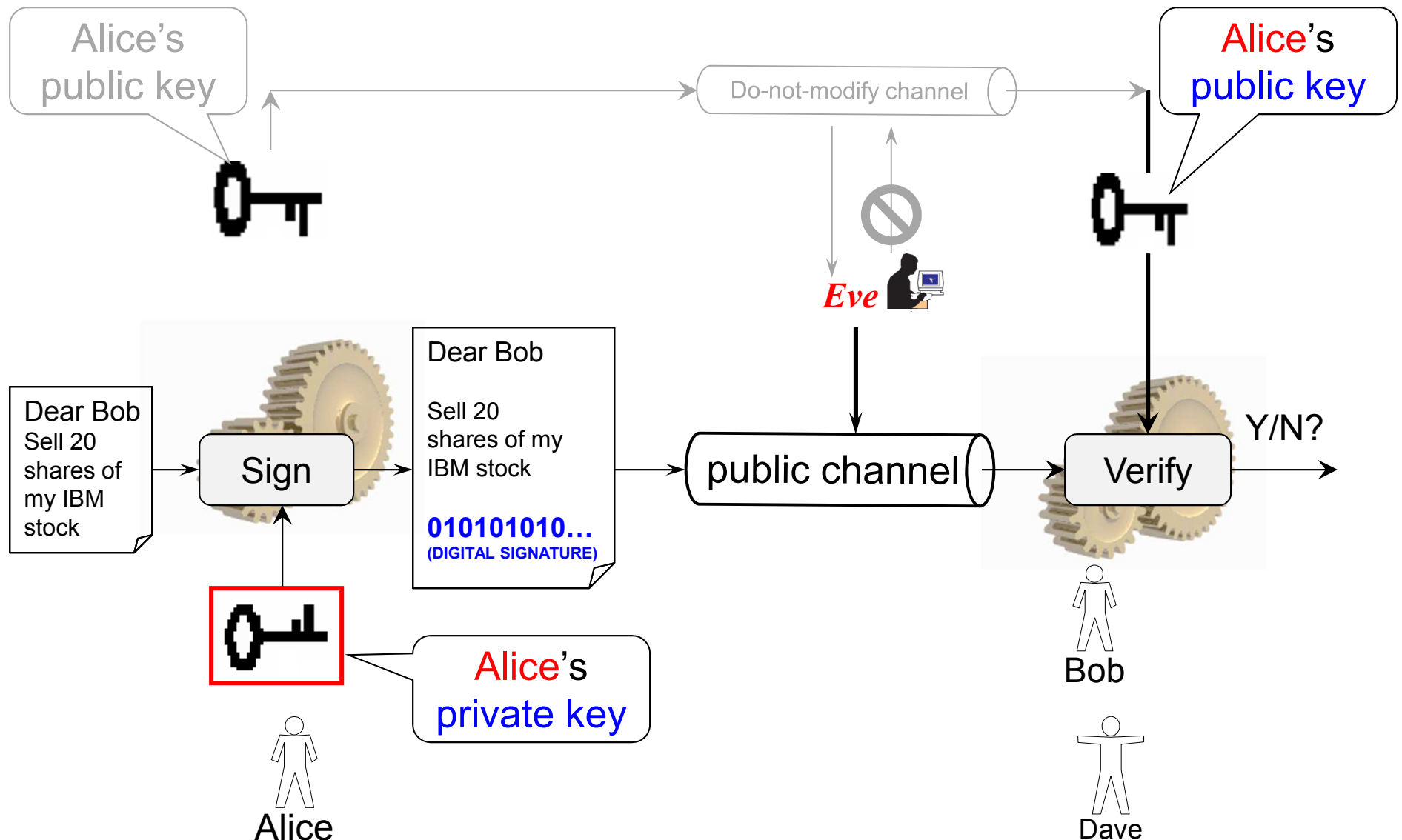




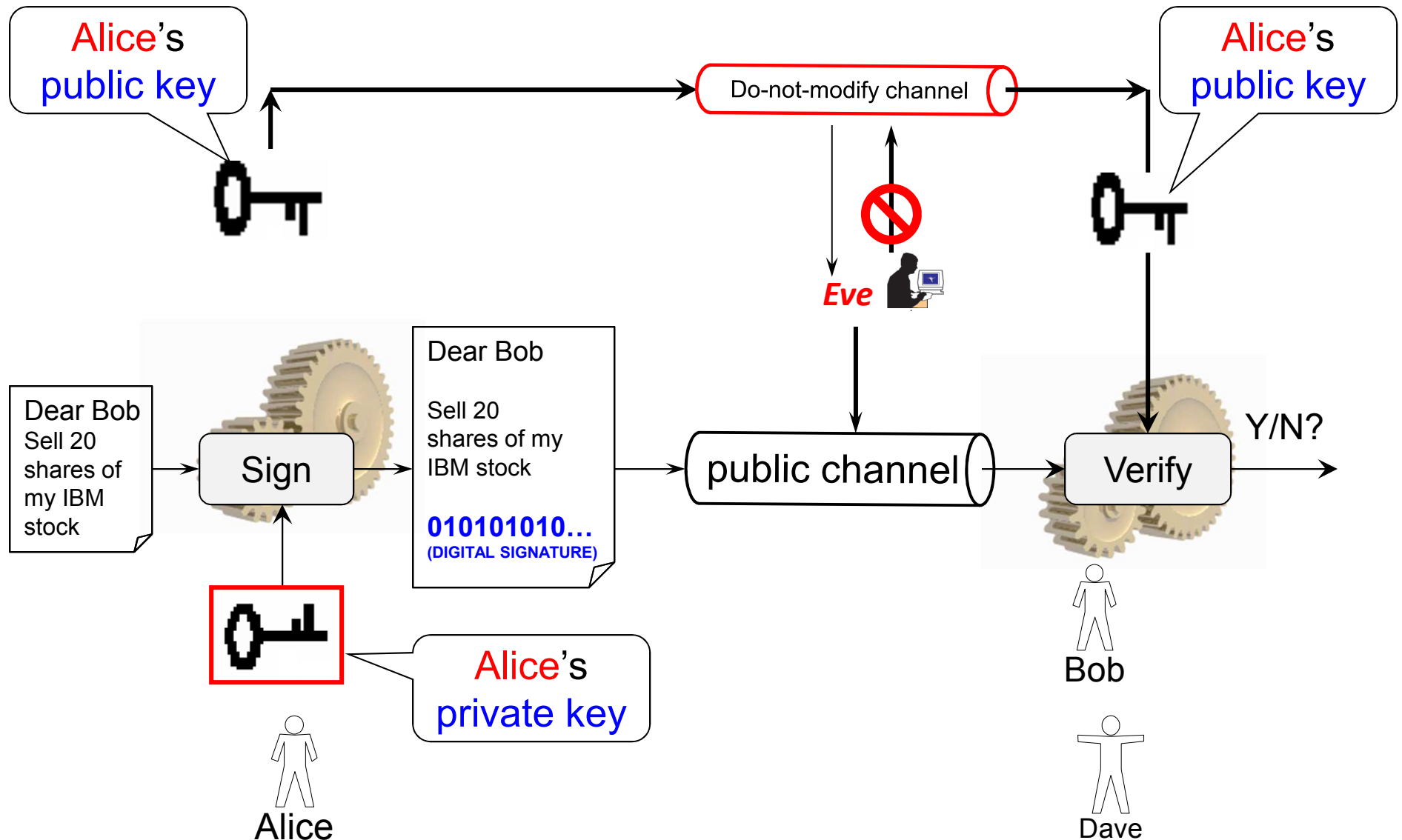
# Public Key Digital Signature



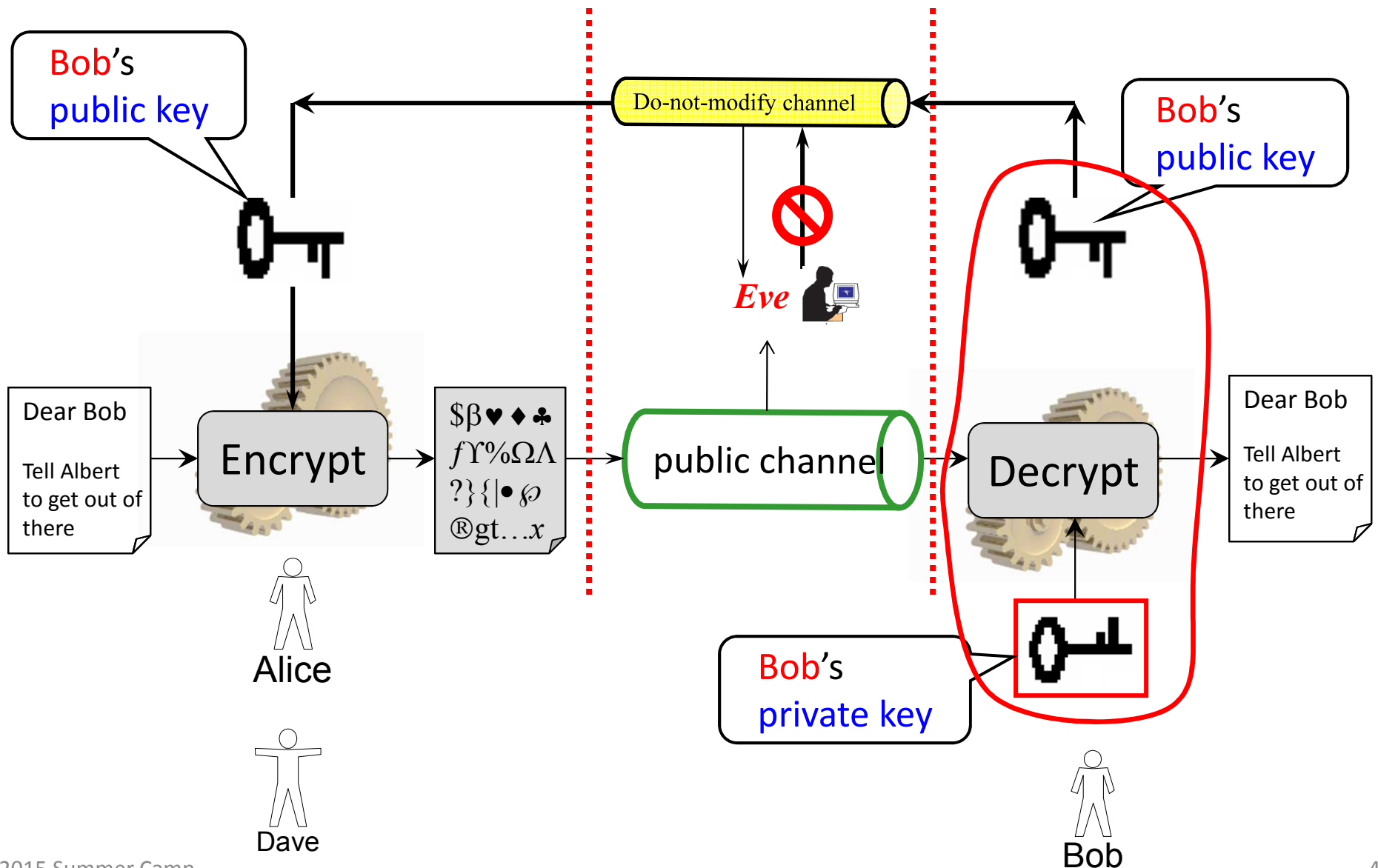
# Public Key Digital Signature



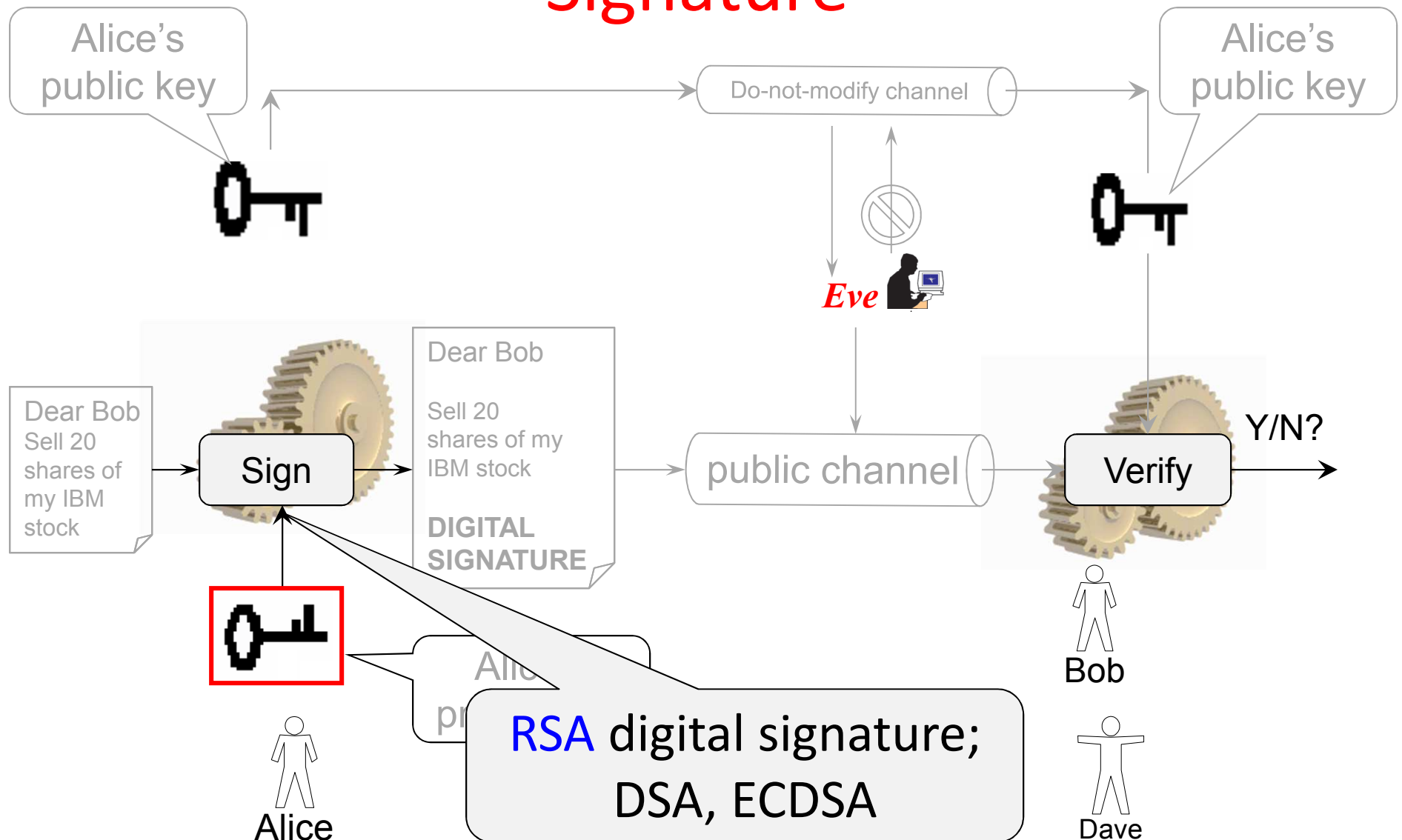
# Public Key Digital Signature



# 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



```
bdf9b90c91d65ae34c481e40  
ec8eb57575b5030afb01bd8f  
544b240d69f5f56b801be1e8  
8f75dc2acd12924e3622bb50  
5f4f845f7ac262f85cf6584a  
01c866e3
```

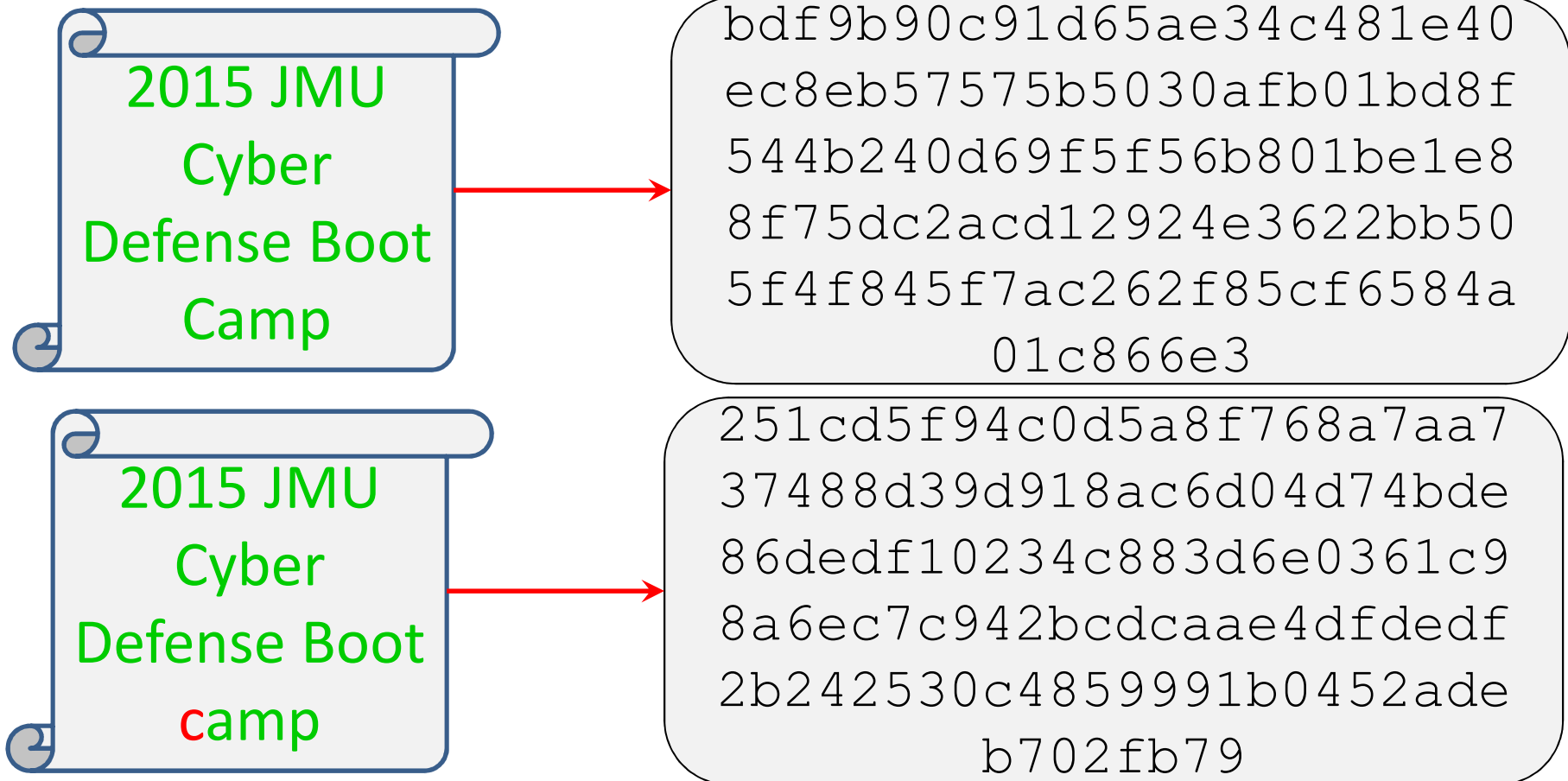


# Cryptographic Hash Function

- 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



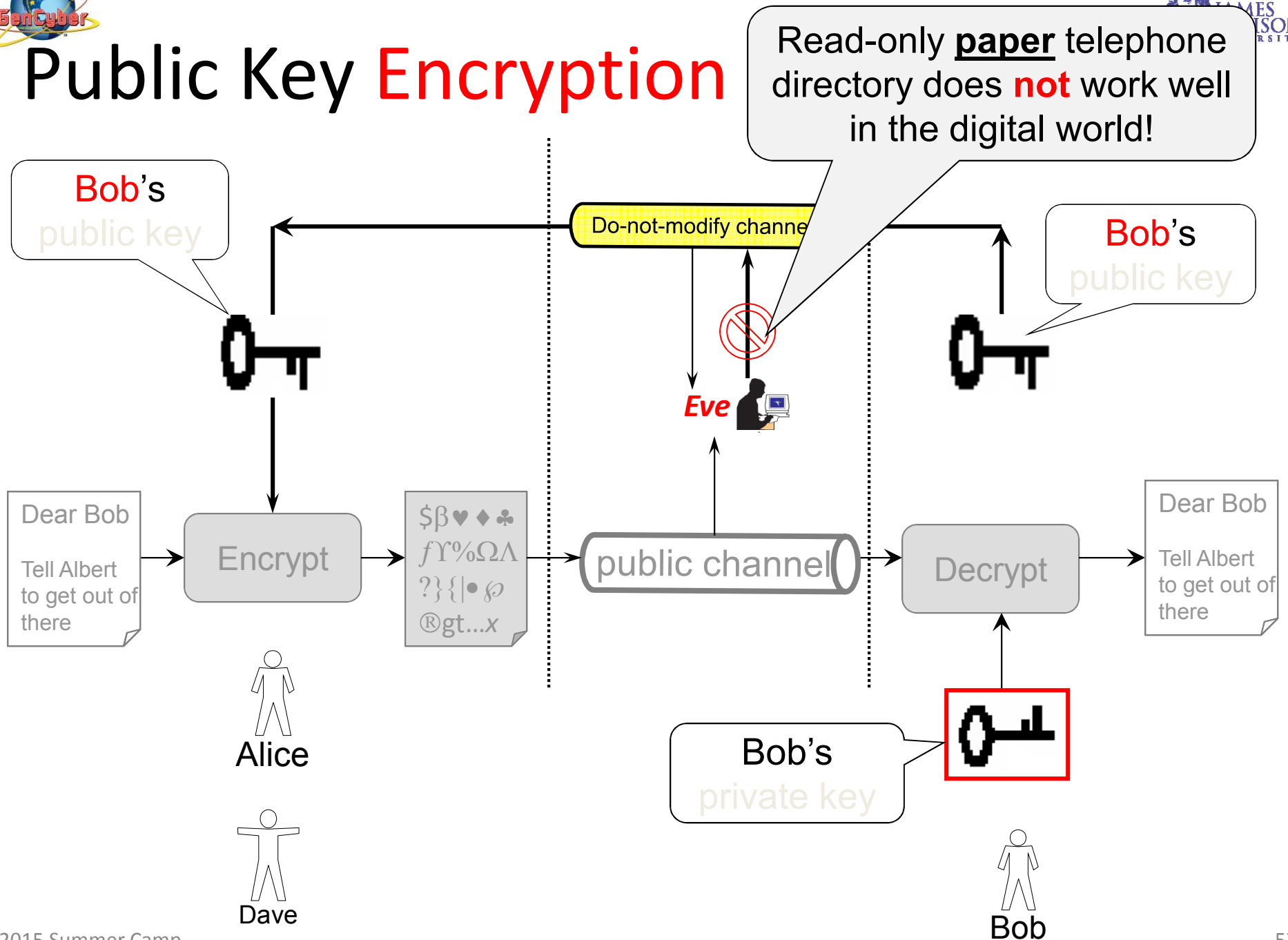


# Road Map

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

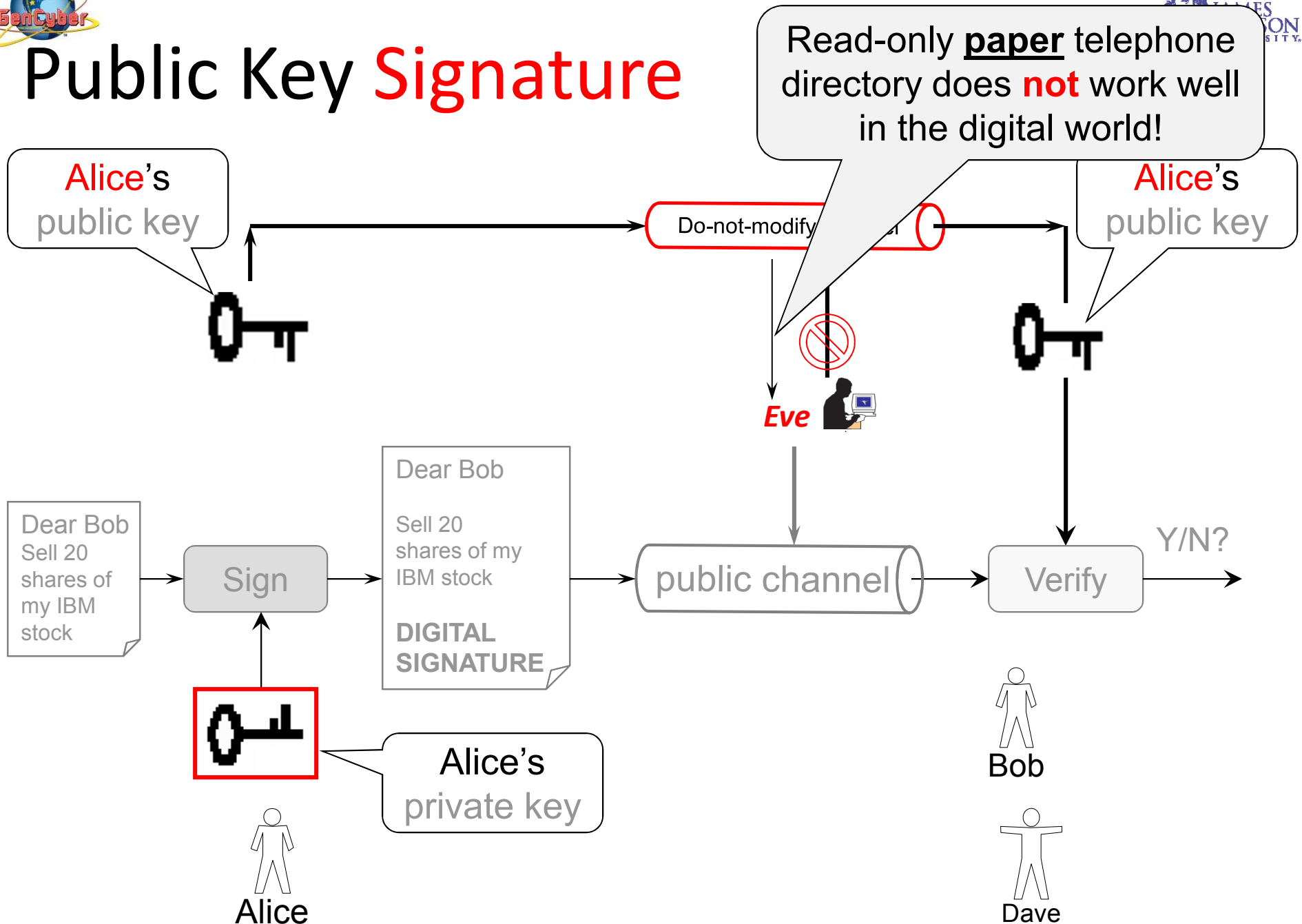


# Public Key Encryption

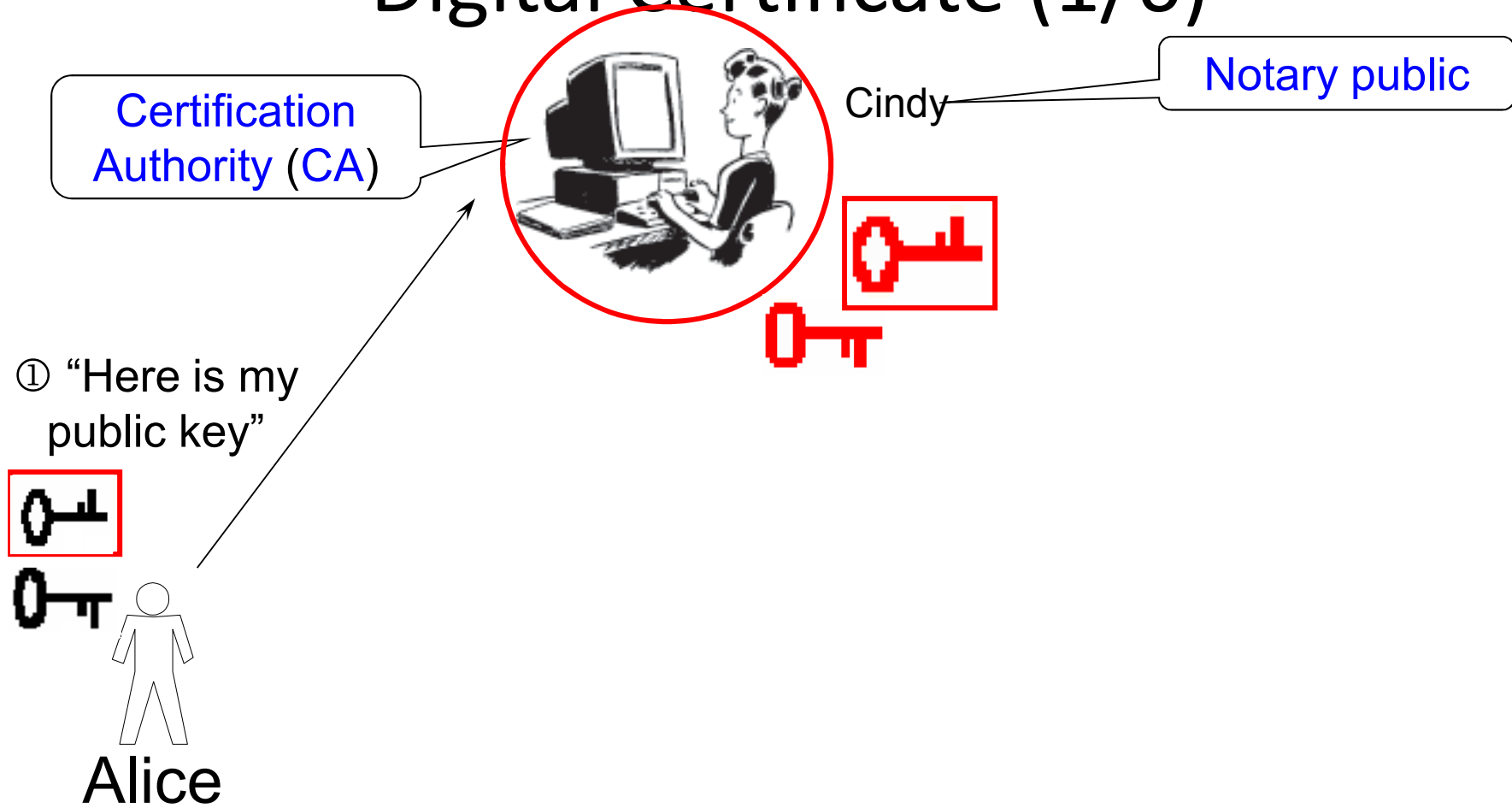




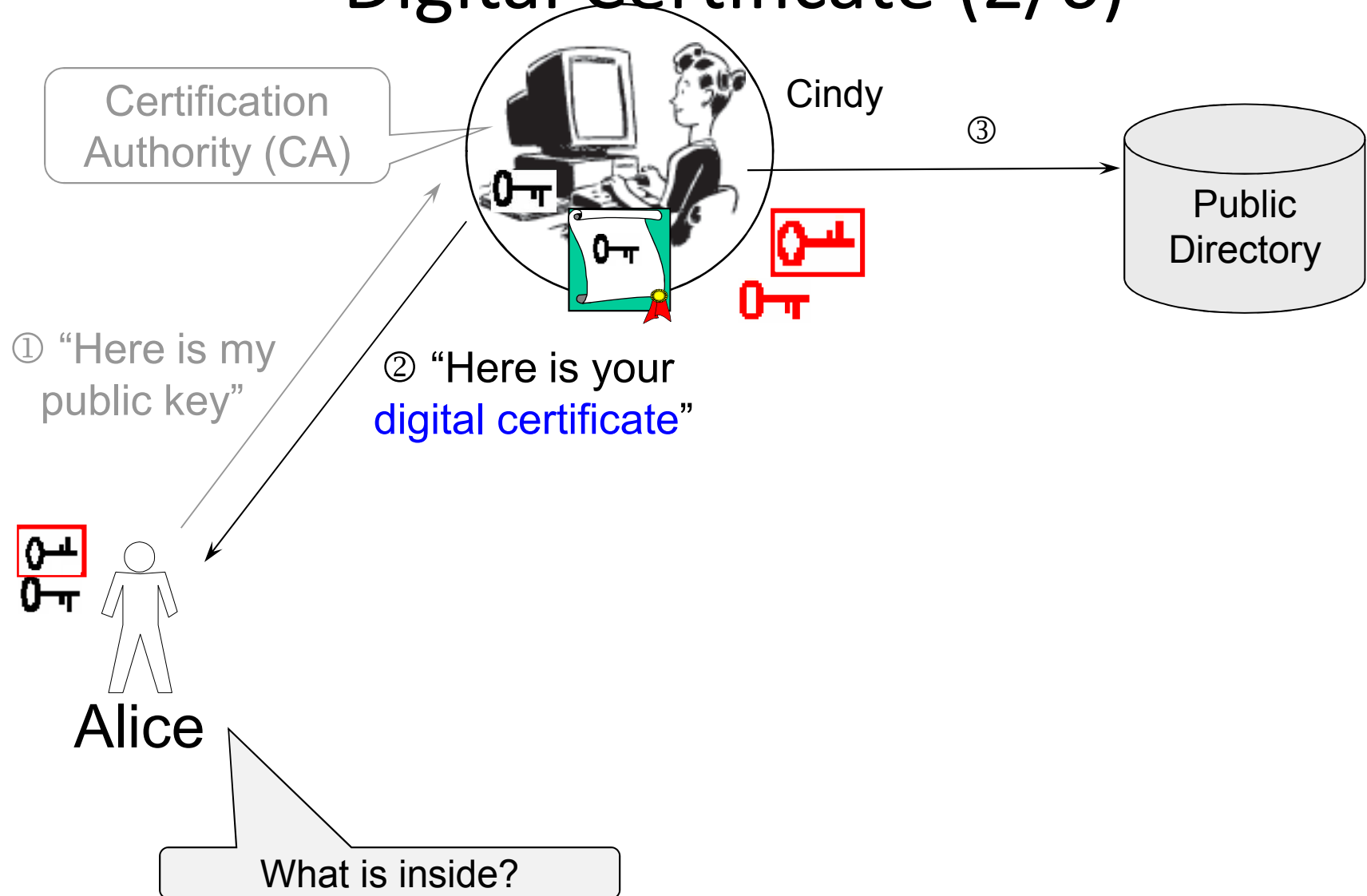
# Public Key Signature



# Digital Certificate (1/6)

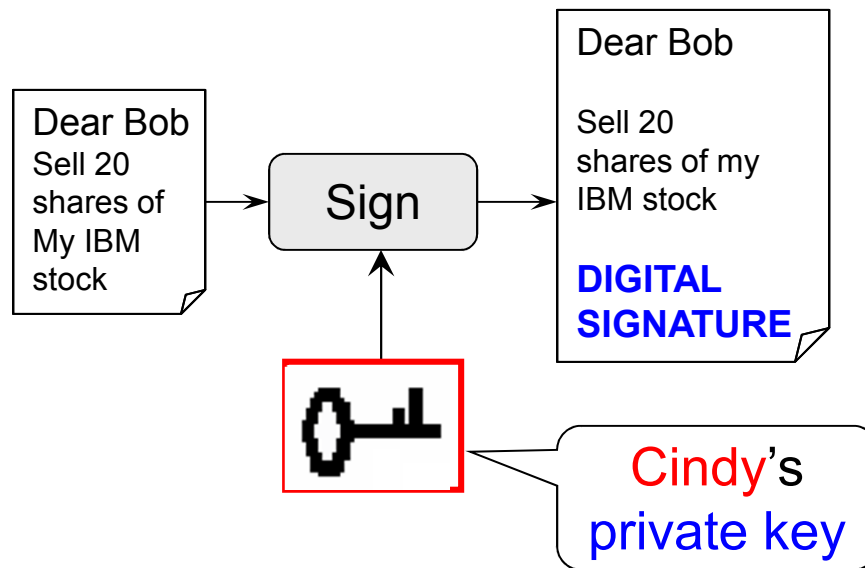


# Digital Certificate (2/6)



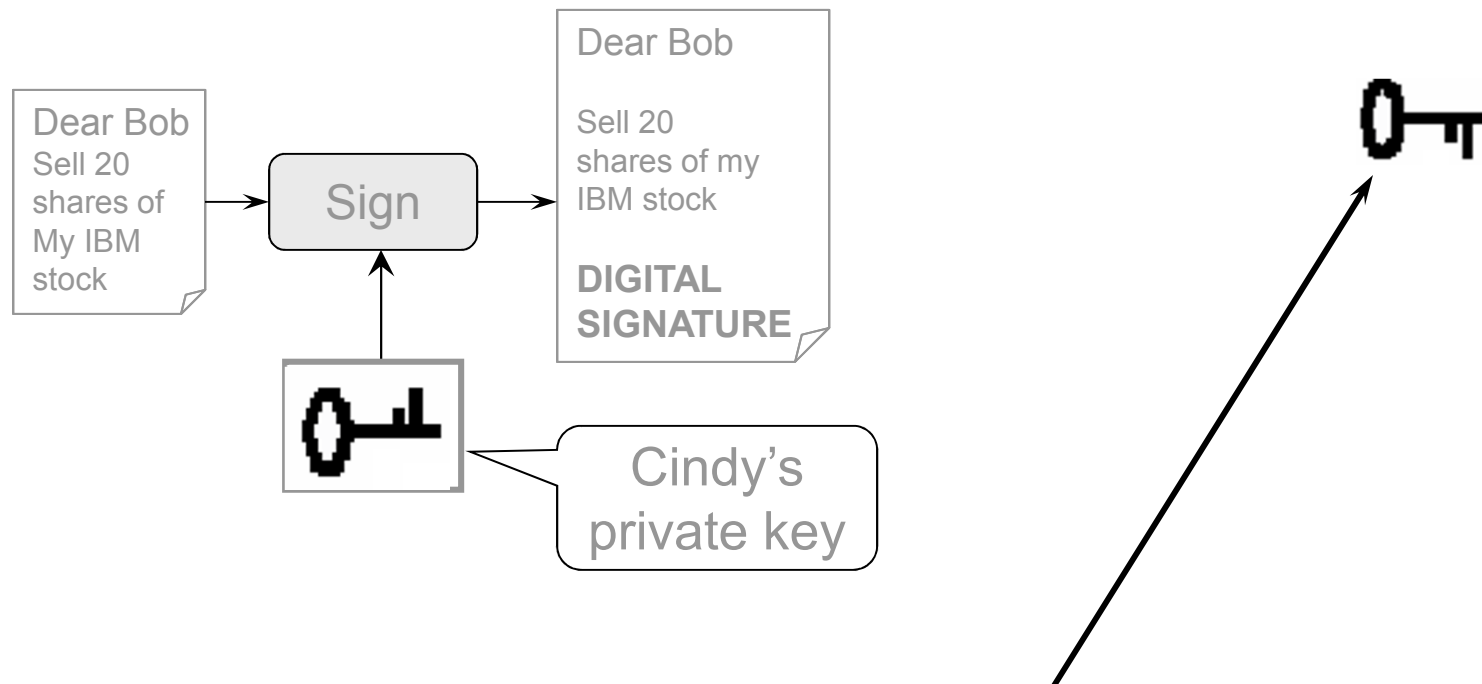


# Digital Certificate (3/6)



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

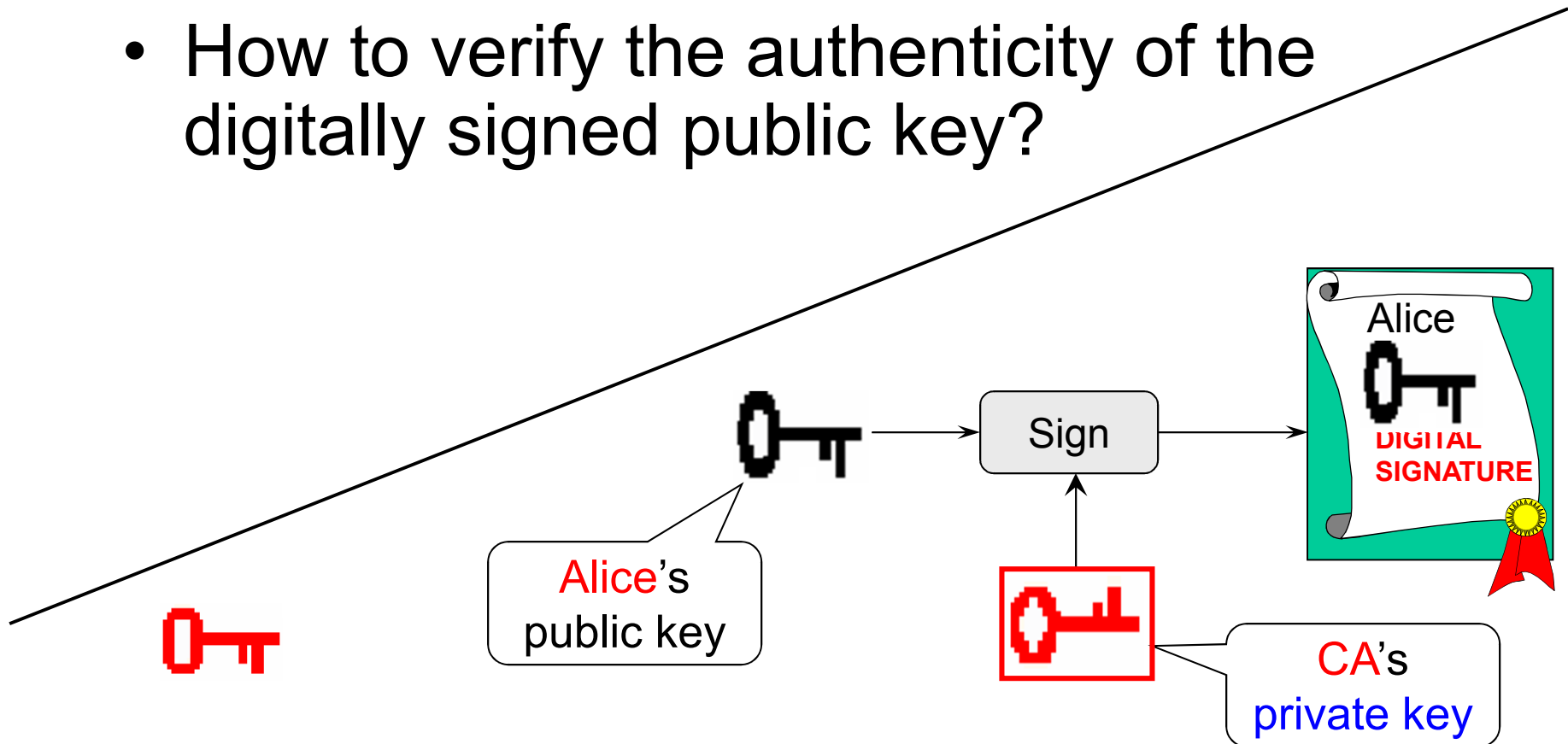
## Digital Certificate (4/6)



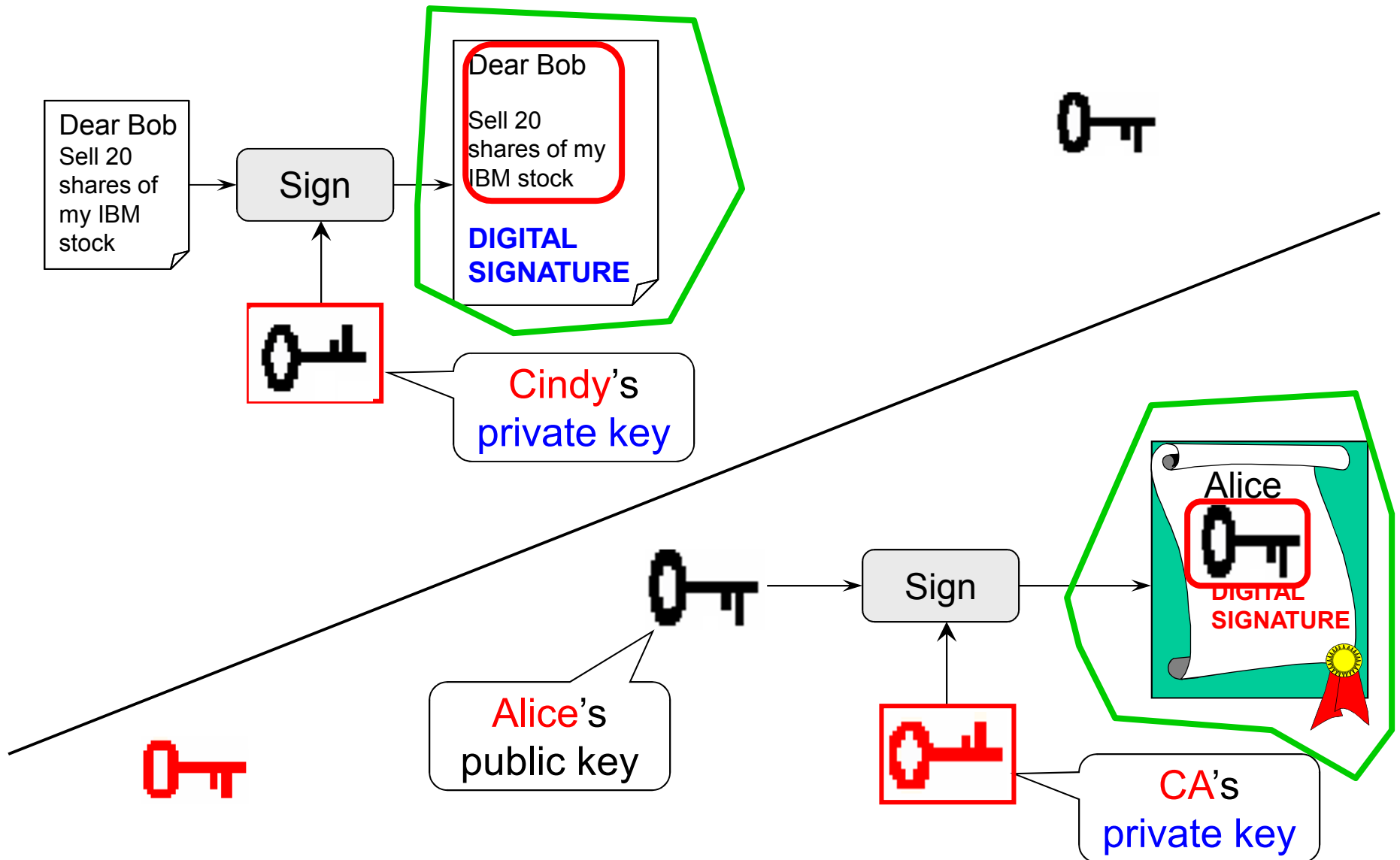
- You need the signer's public key!
- What if you mistook a bad guy's public key as the signer's public key?

# 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

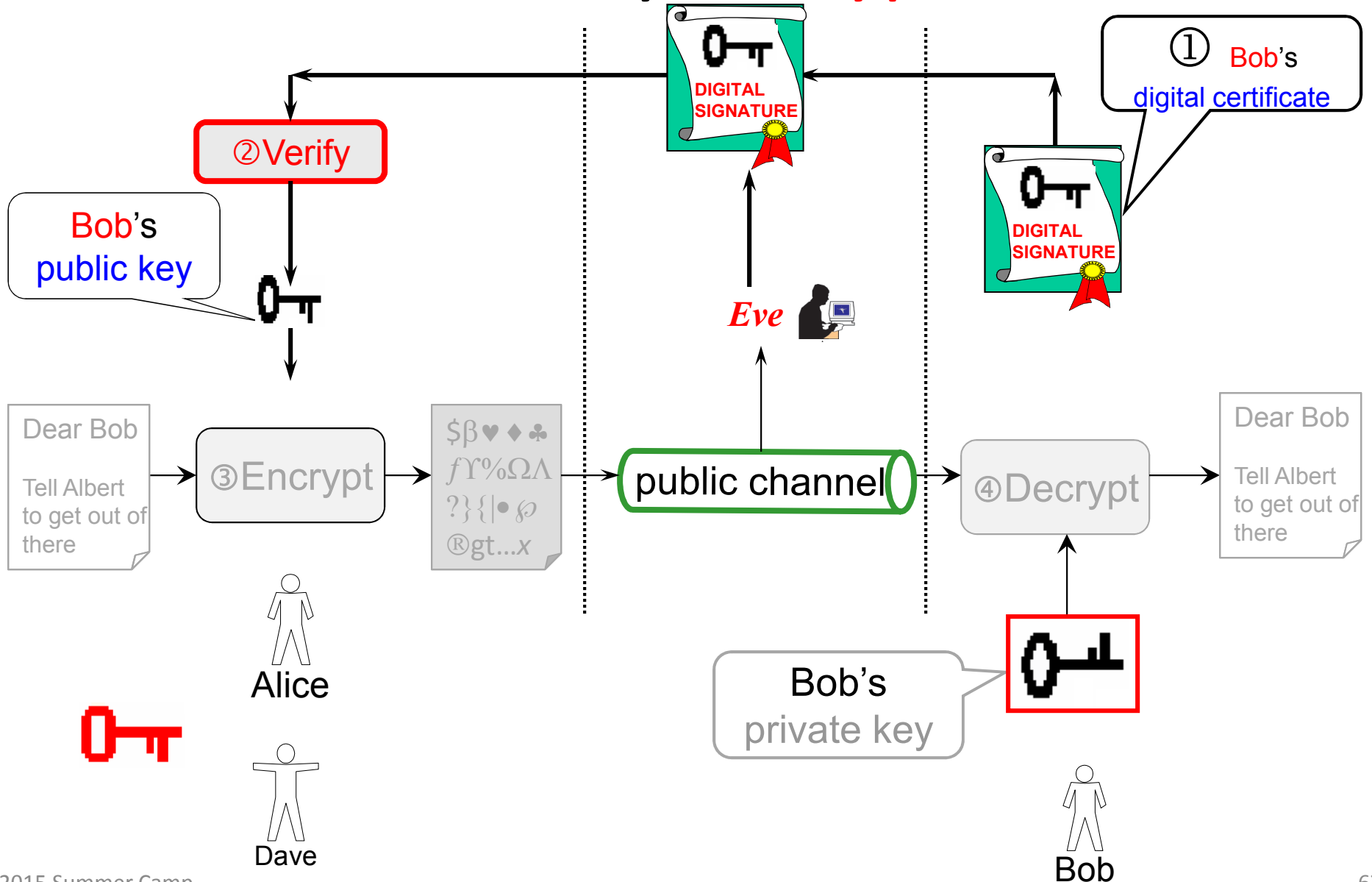




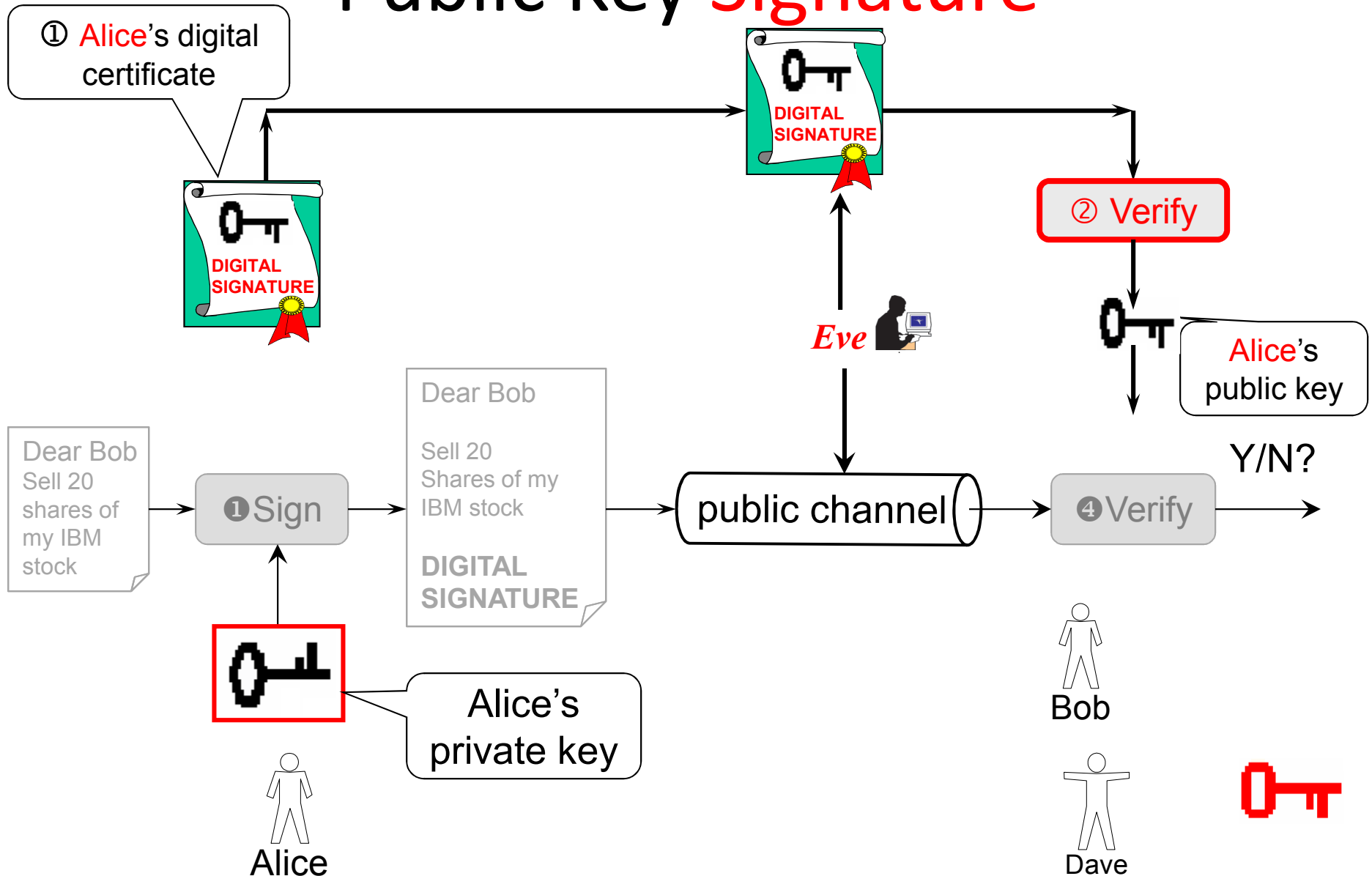
# Stealing a digital certificate?

- Stealing a private key

# 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 ...



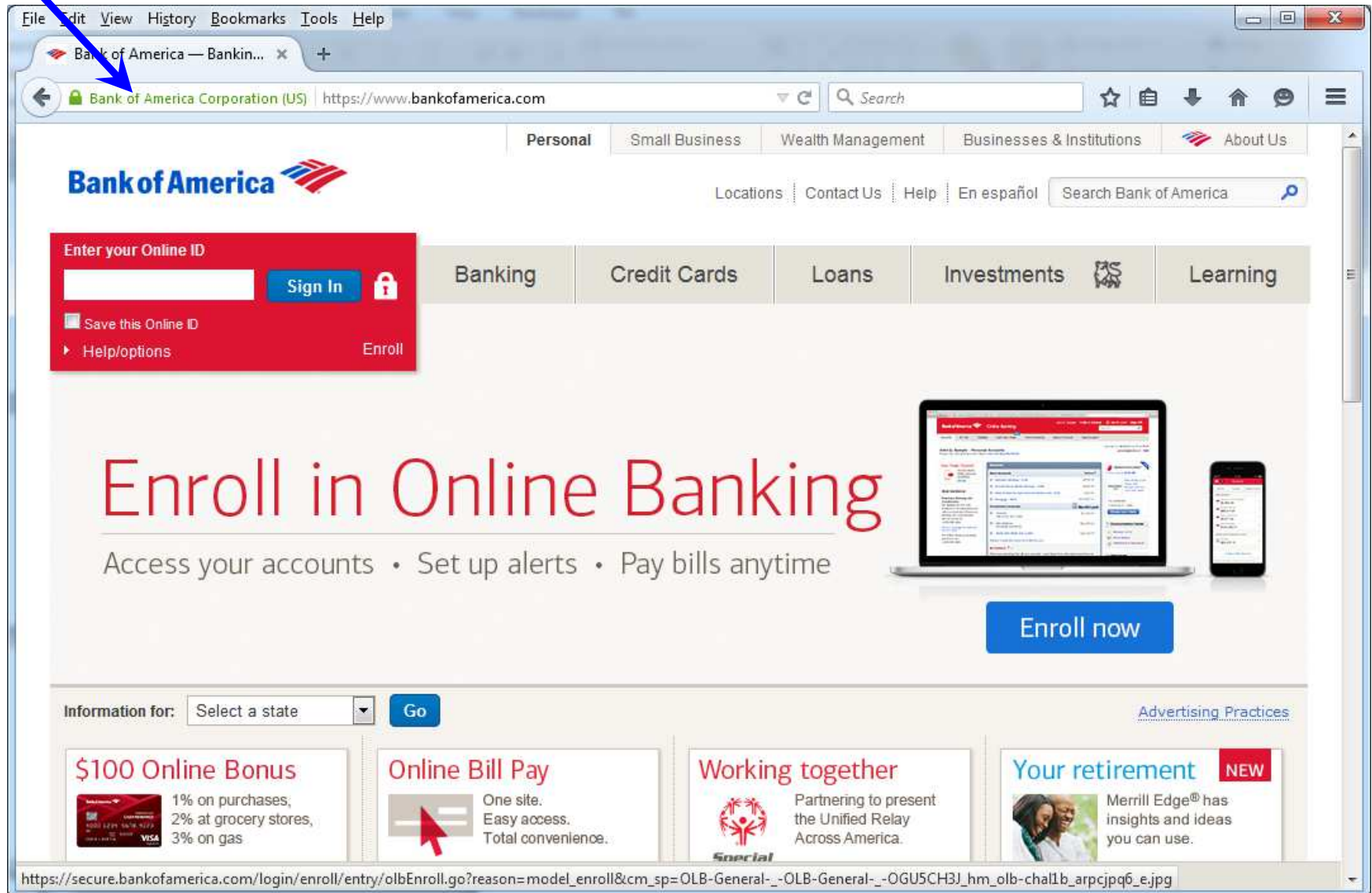


# Road Map

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



# What is This?



File Edit View History Bookmarks Tools Help

Bank of America — Bankin... x

Bank of America Corporation (US) https://www.bankofamerica.com Search

You are connected to **bankofamerica.com** which is run by **Bank of America Corporation** Chicago Illinois, US Verified by: Symantec Corporation The connection to this website is secure.

**BOA is Alice**

**Symantec is CA**

More Information...

# Enroll in Online Banking

Access your accounts • Set up alerts • Pay bills anytime

Enroll now

Information for: Select a state Go

**\$100 Online Bonus**  
1% on purchases,  
2% at grocery stores,  
3% on gas

**Online Bill Pay**  
One site.  
Easy access.  
Total convenience.

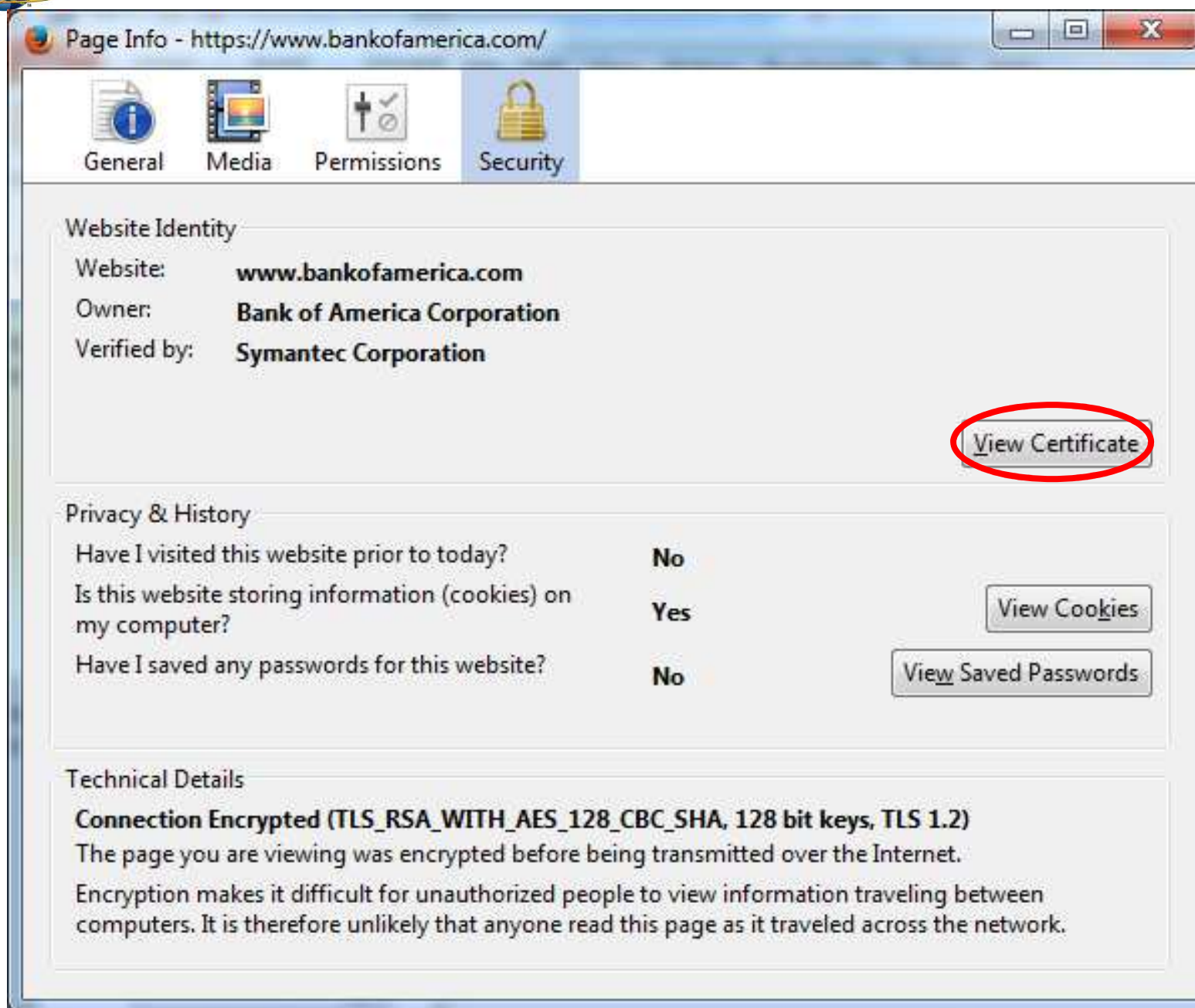
**Working together**  
Partnering to present  
the Unified Relay  
Across America.

**Your retirement**  
Merrill Edge  
insights  
you can

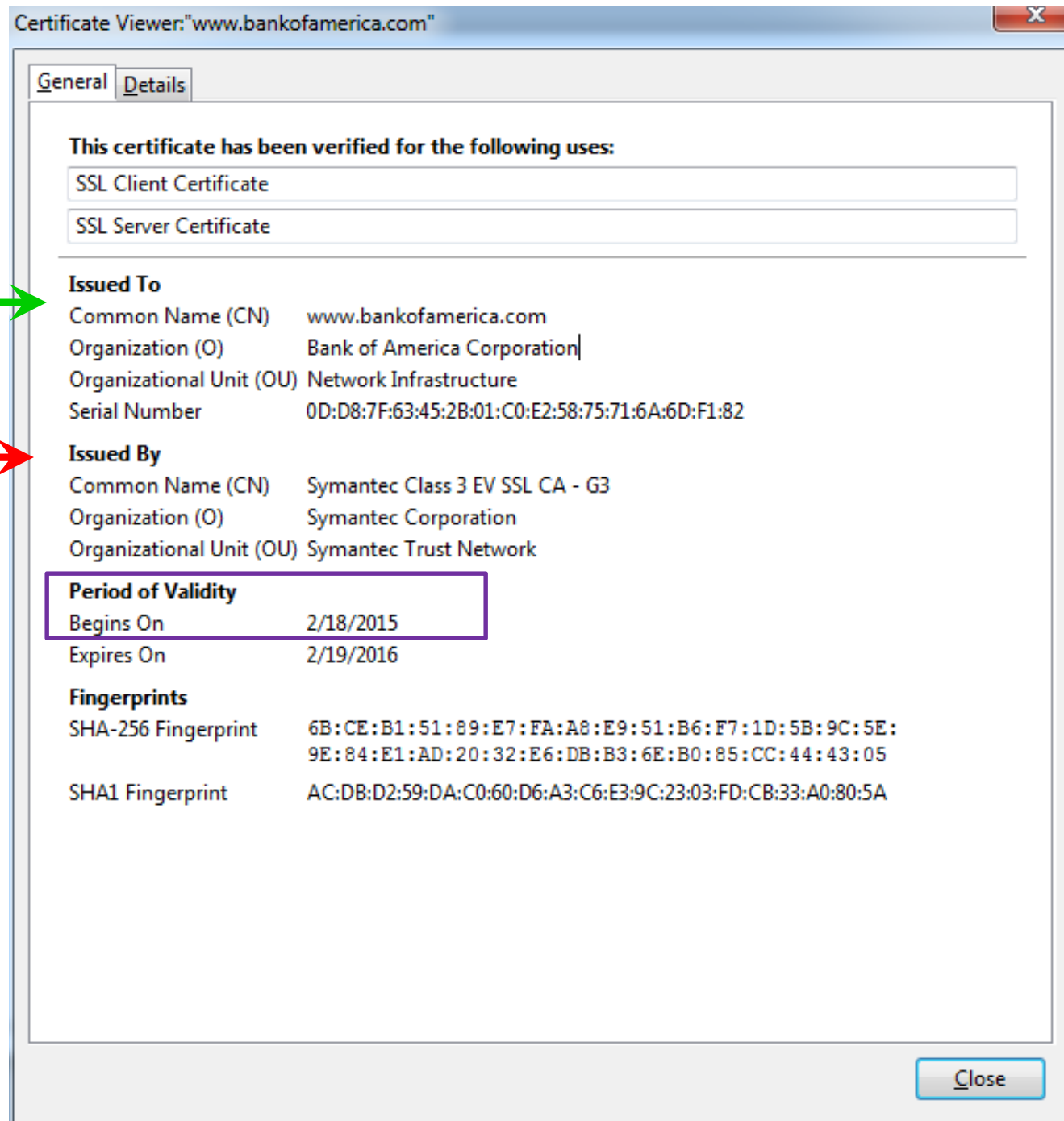
Share website feedback

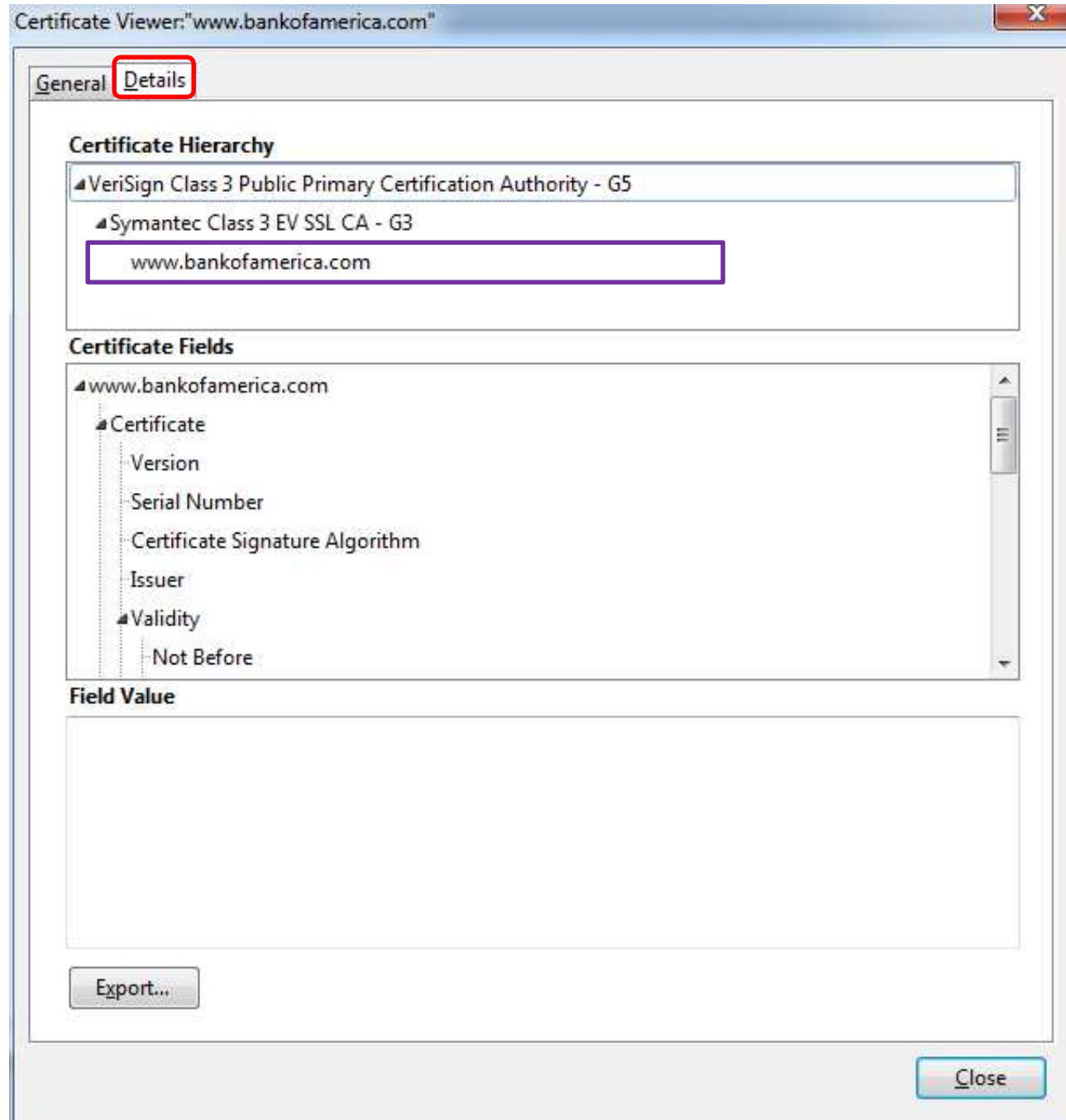
2015 Summer Camp

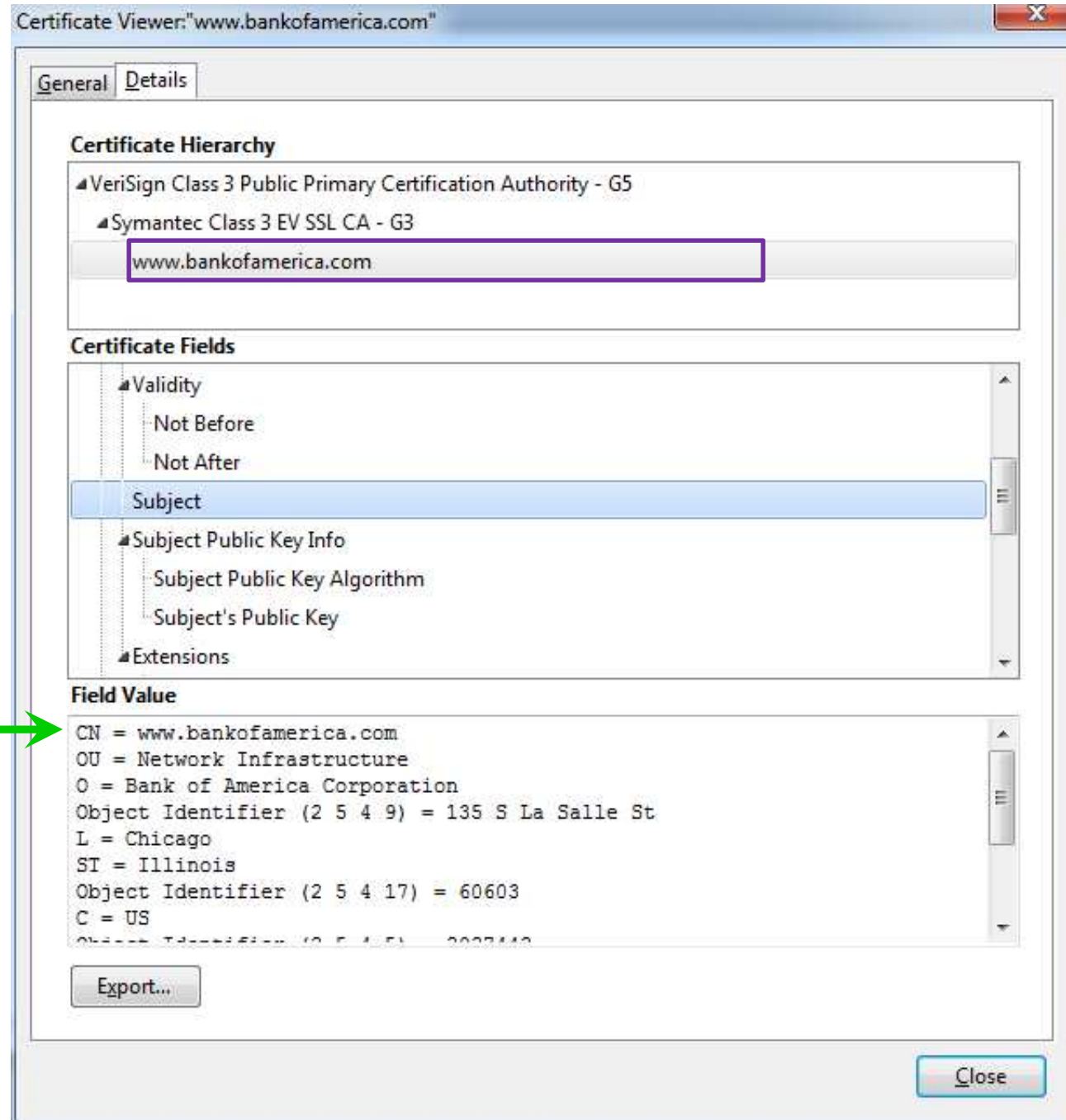
72



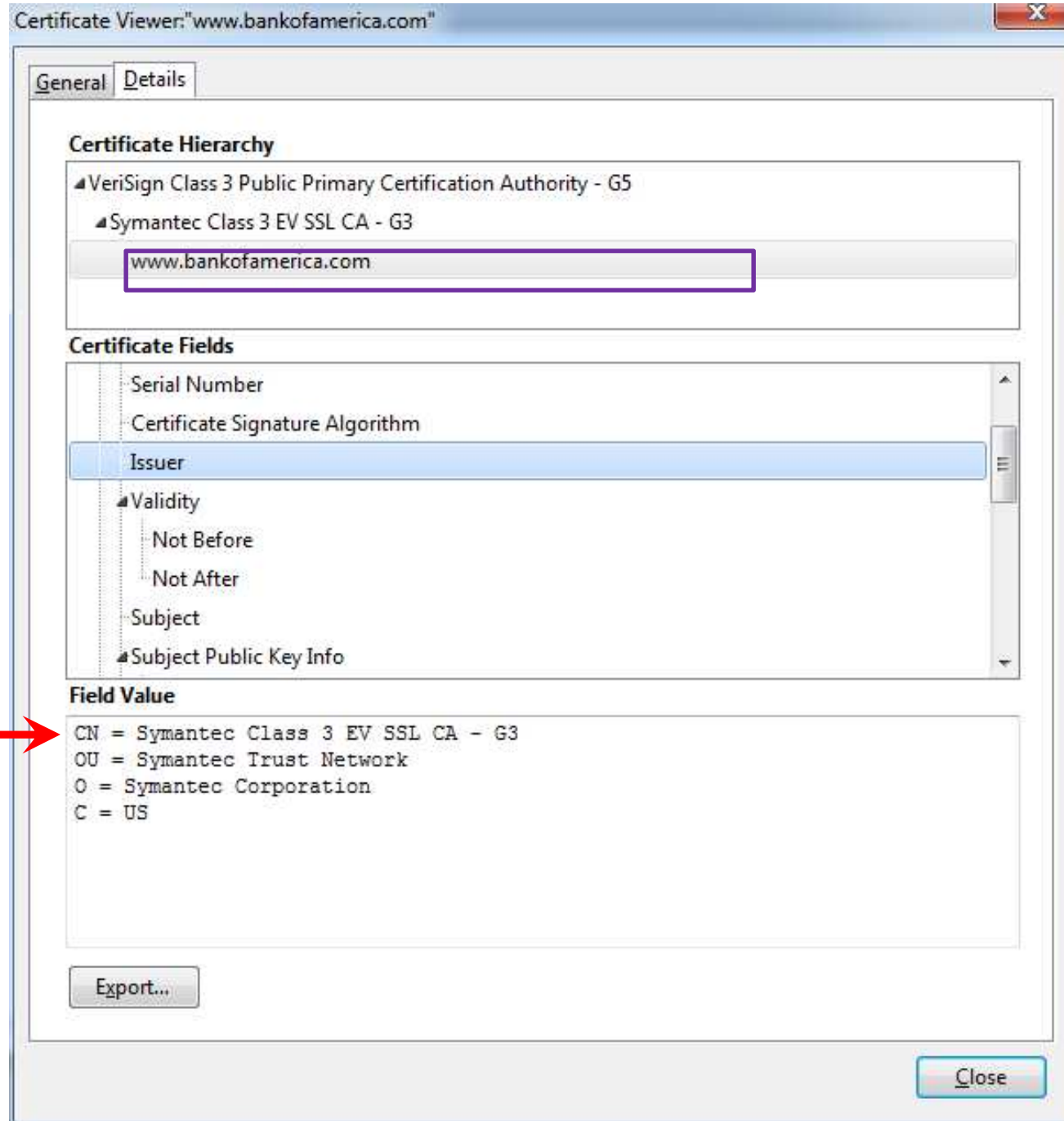


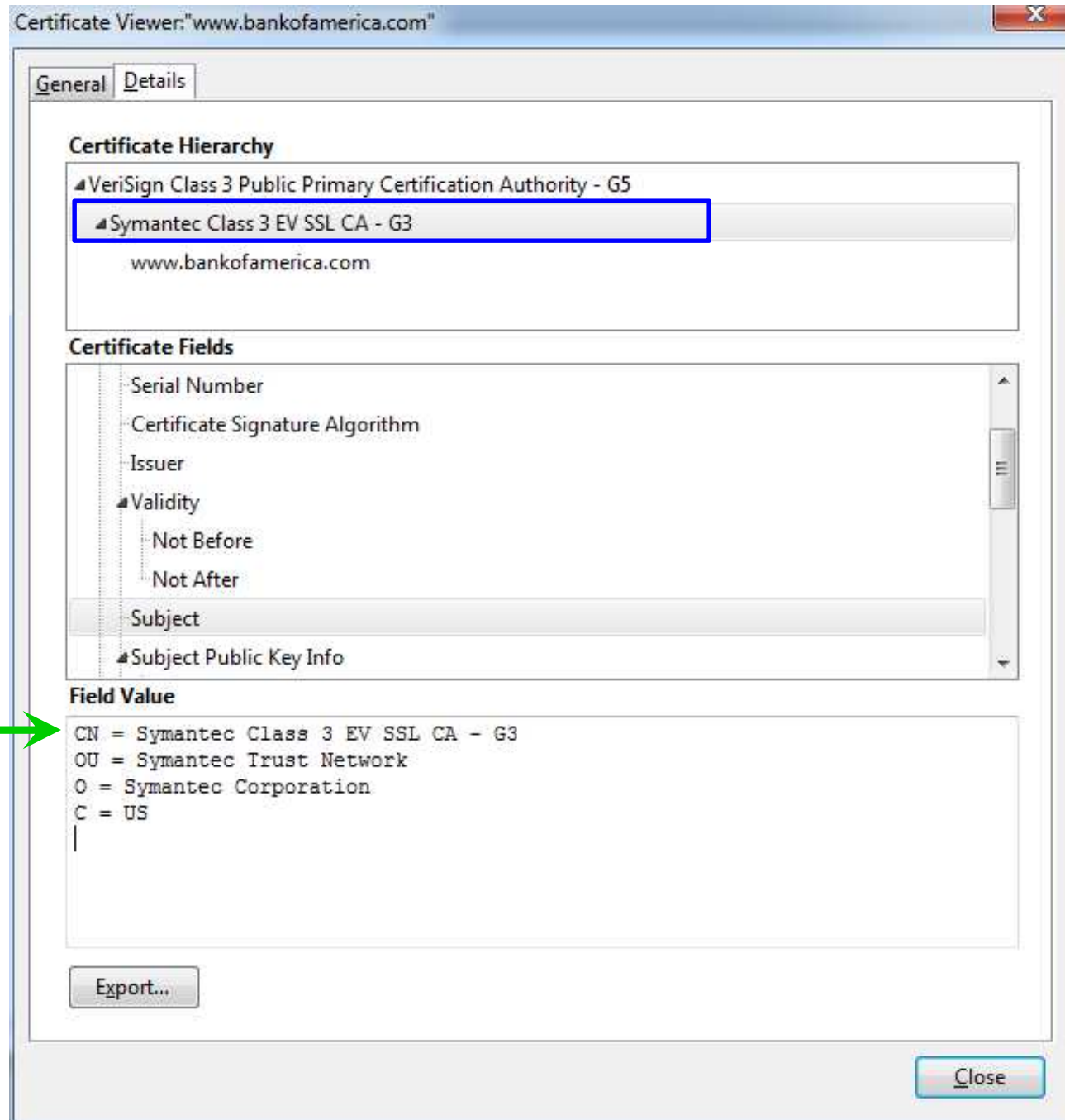


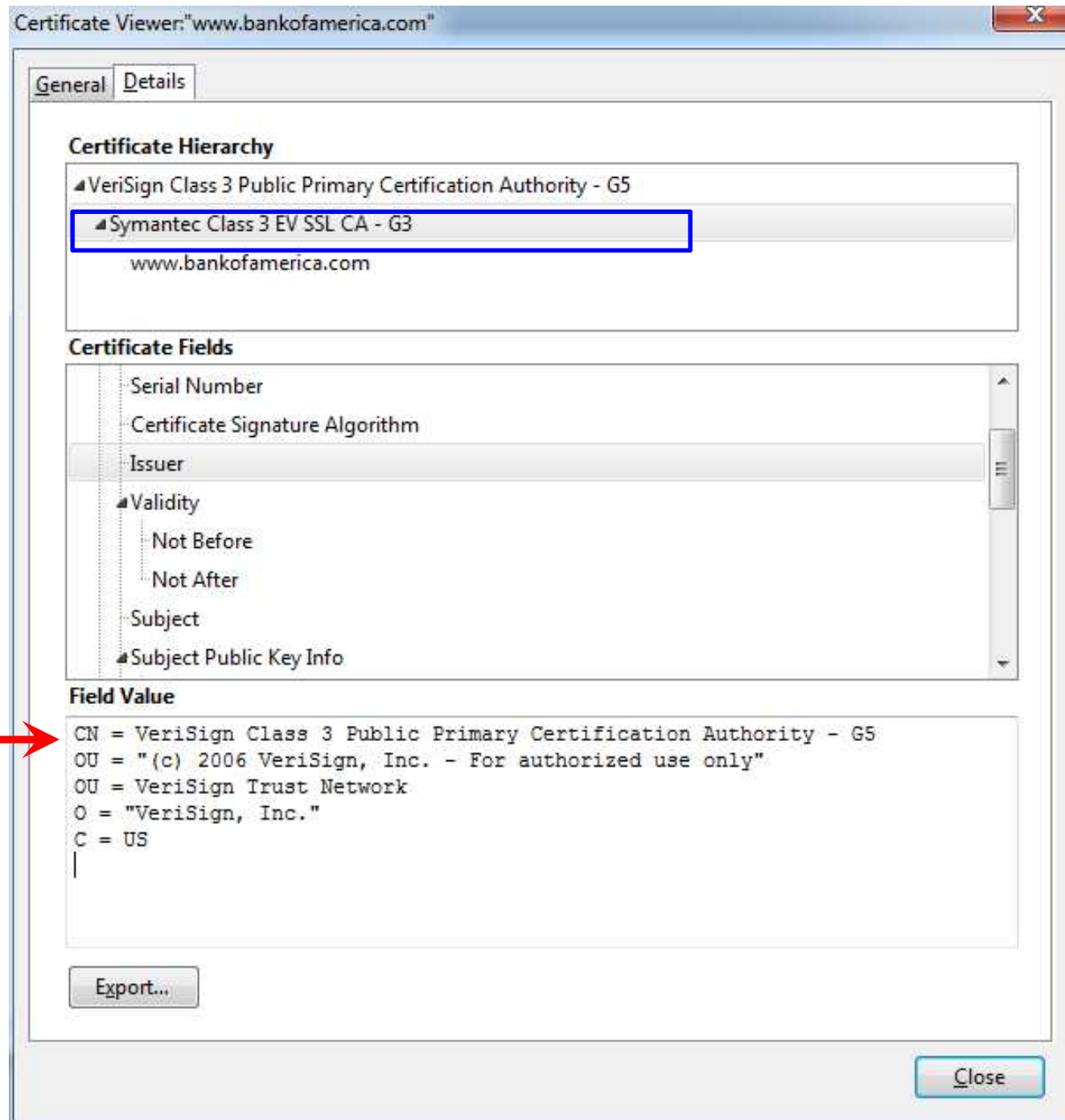


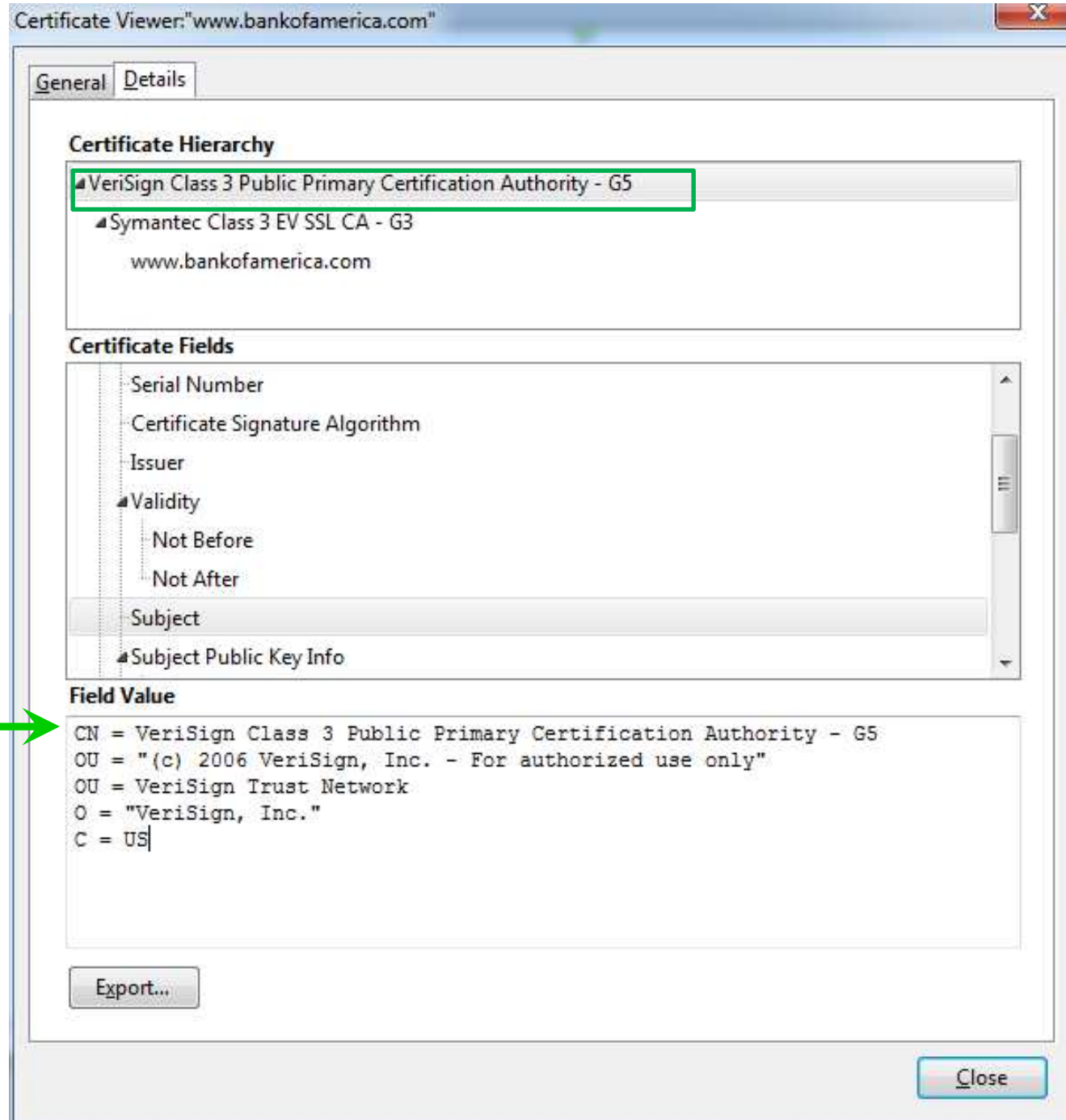


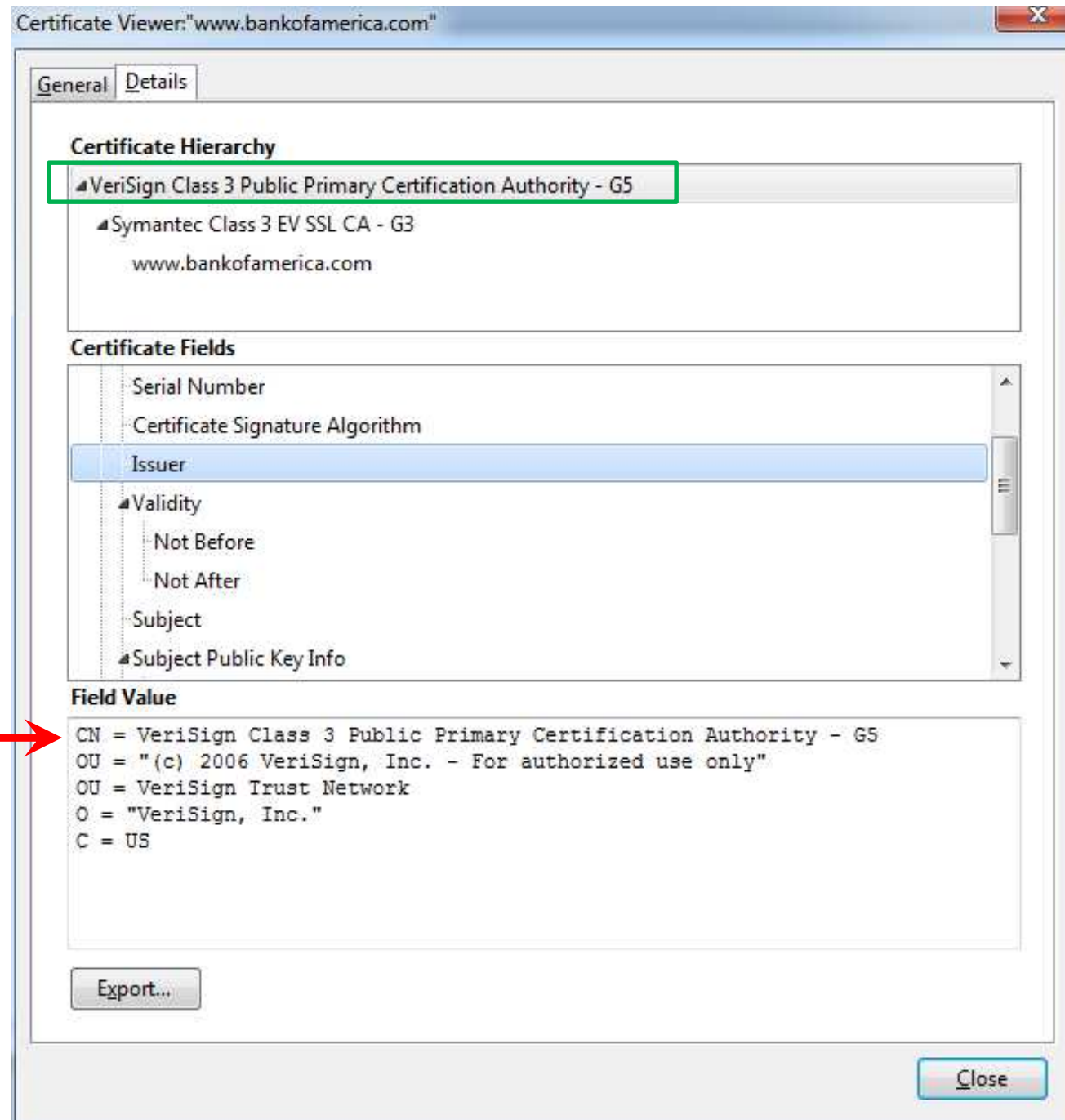














Page Info - https://www.bankofamerica.com/

General Media Permissions **Security**

### Website Identity

Website: **www.bankofamerica.com**  
Owner: **Bank of America Corporation**  
Verified by: **Symantec Corporation**

[View Certificate](#)

### Privacy & History

Have I visited this website prior to today?	<b>No</b>	
Is this website storing information (cookies) on my computer?	<b>Yes</b>	<a href="#">View Cookies</a>
Have I saved any passwords for this website?	<b>No</b>	<a href="#">View Saved Passwords</a>

### Technical Details

**Connection Encrypted (TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA, 128 bit keys, TLS 1.2)**

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

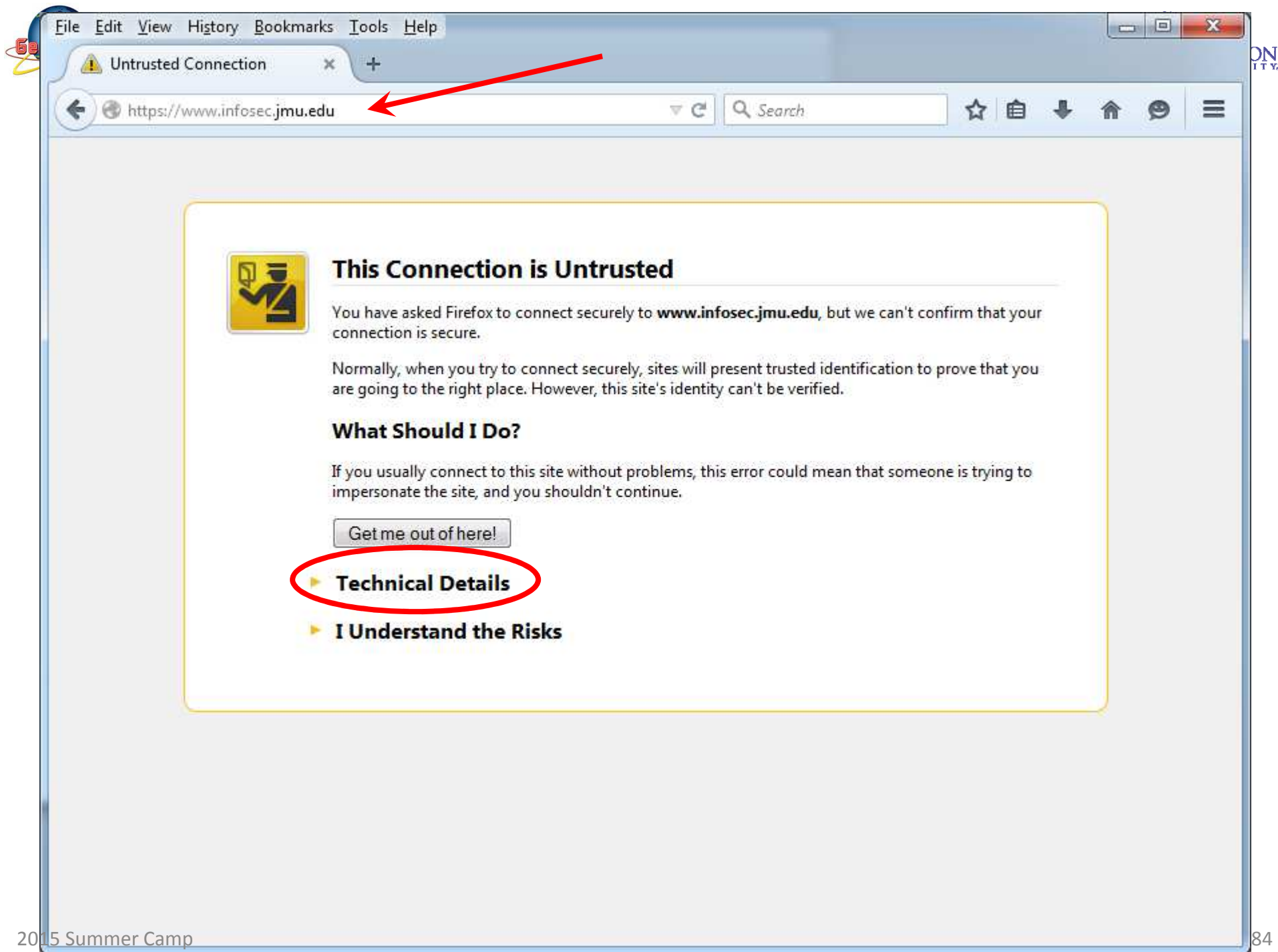


The image shows a screenshot of the Bank of America website. A red box highlights the "Enter your Online ID" field, which contains the text "John Doe". A red arrow points from this field to a diagram on the right. The diagram shows a person labeled "Alice" at the bottom, a server labeled "Server" at the top, and a large grey cylinder labeled "Secure Channel" in the middle. A red arrow points from Alice to the "Secure Channel", and another red arrow points from the "Secure Channel" to the Server. A label "PII" is placed near Alice, indicating that the information being transmitted is Personally Identifiable Information. Below the main website screenshot, there is a smaller screenshot of a browser's security information window. It shows the website identity as "www.bankofamerica.com" and the owner as "Bank of America Corporation". It also displays technical details, including "Connection Encrypted (TLS, RSA, WITH AES, 128 CBC, SHA, 128 bit keys, TLS 1.2)".

File Edit View History Bookmarks Tools Help

Untrusted Connection x +

https://www.infosec.jmu.edu Search



**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**
- ▶ **I Understand the Risks**



File Edit View History Bookmarks Tools Help

Untrusted Connection x +

https://www.infosec.jmu.edu Search

 **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.

▼ **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**

20 85

File Edit View History Bookmarks Tools Help

Untrusted Connection x +

https://www.infosec.jmu.edu Search



### 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!

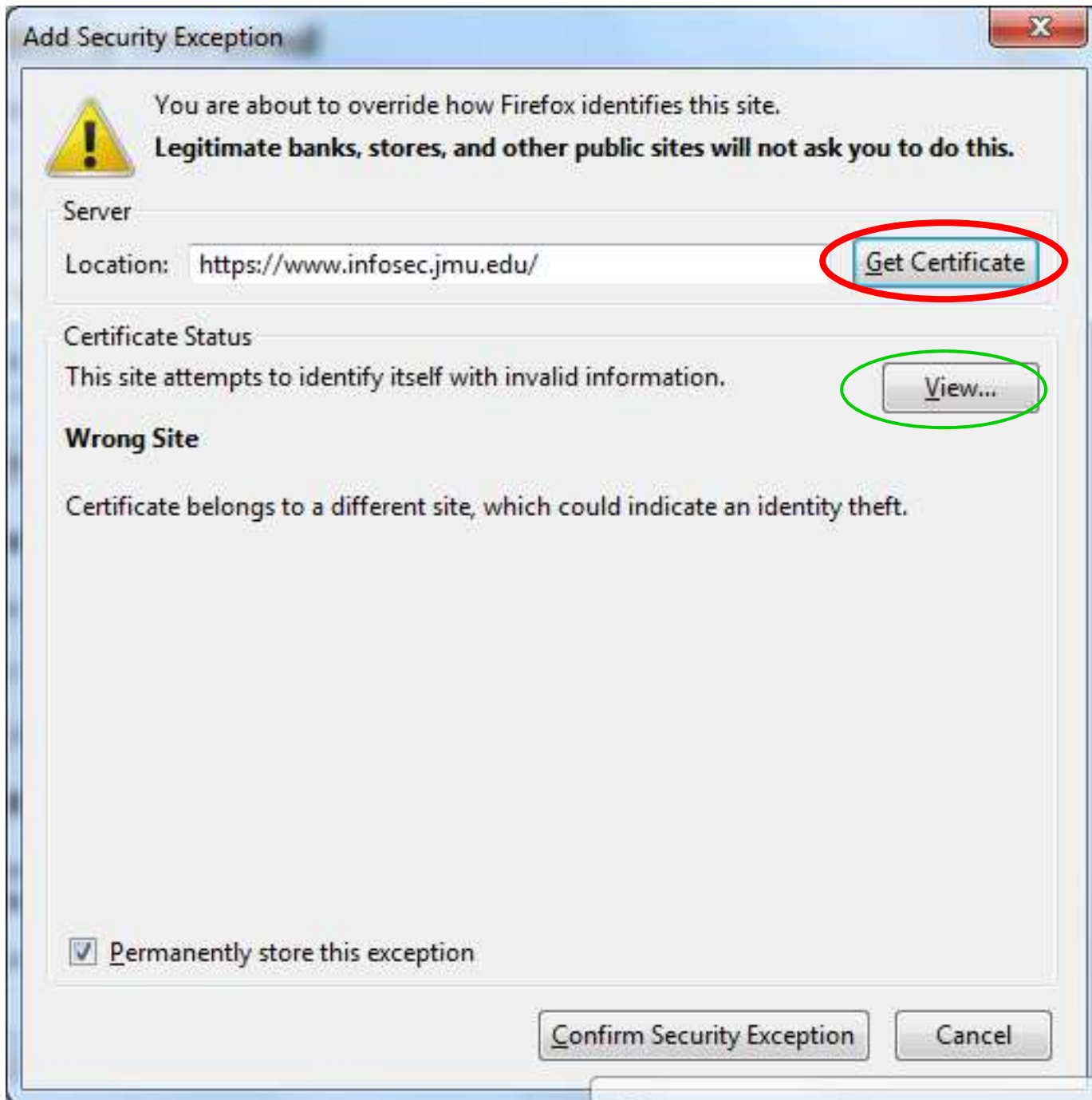
#### Technical Details

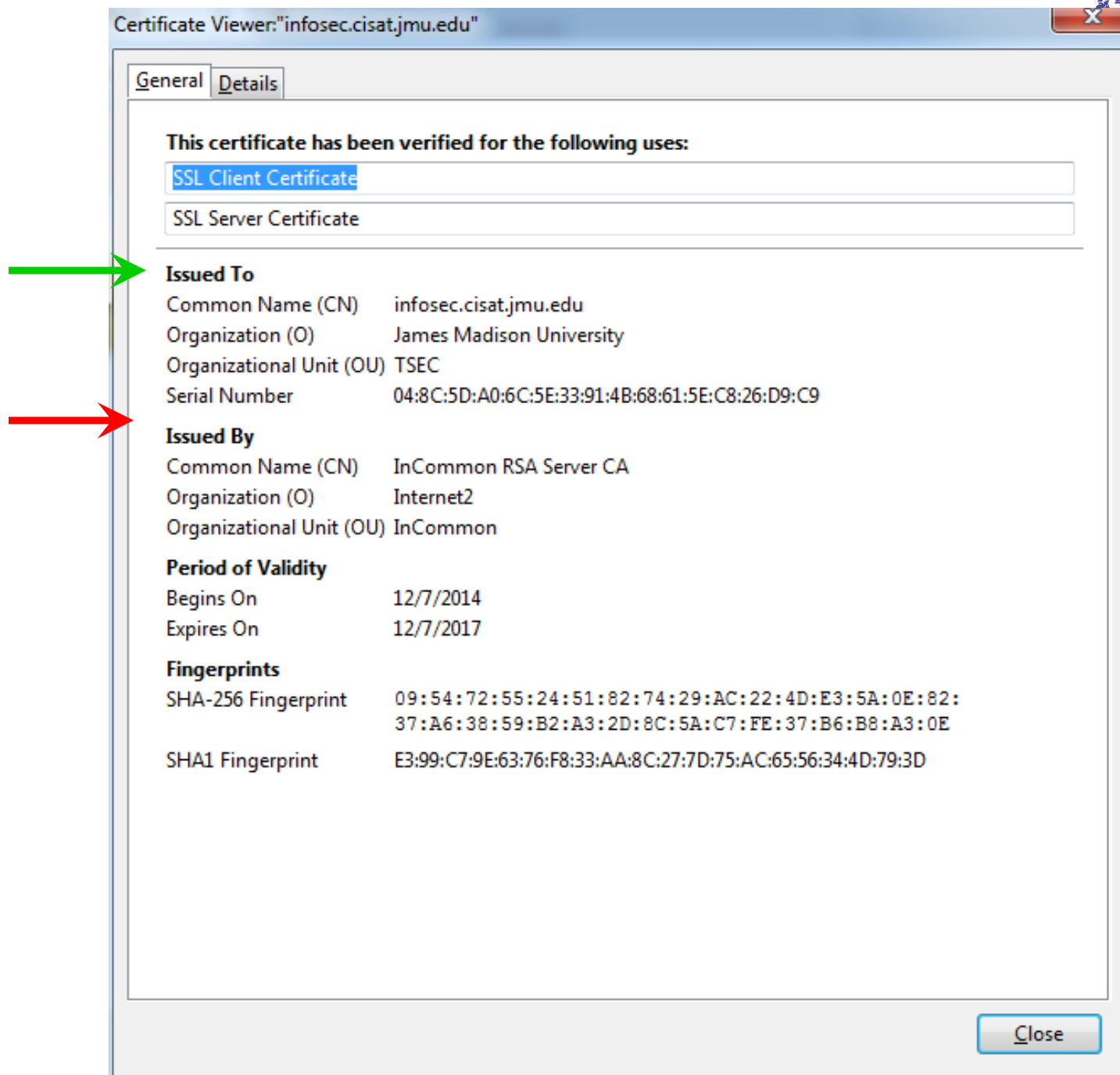
#### I Understand the Risks

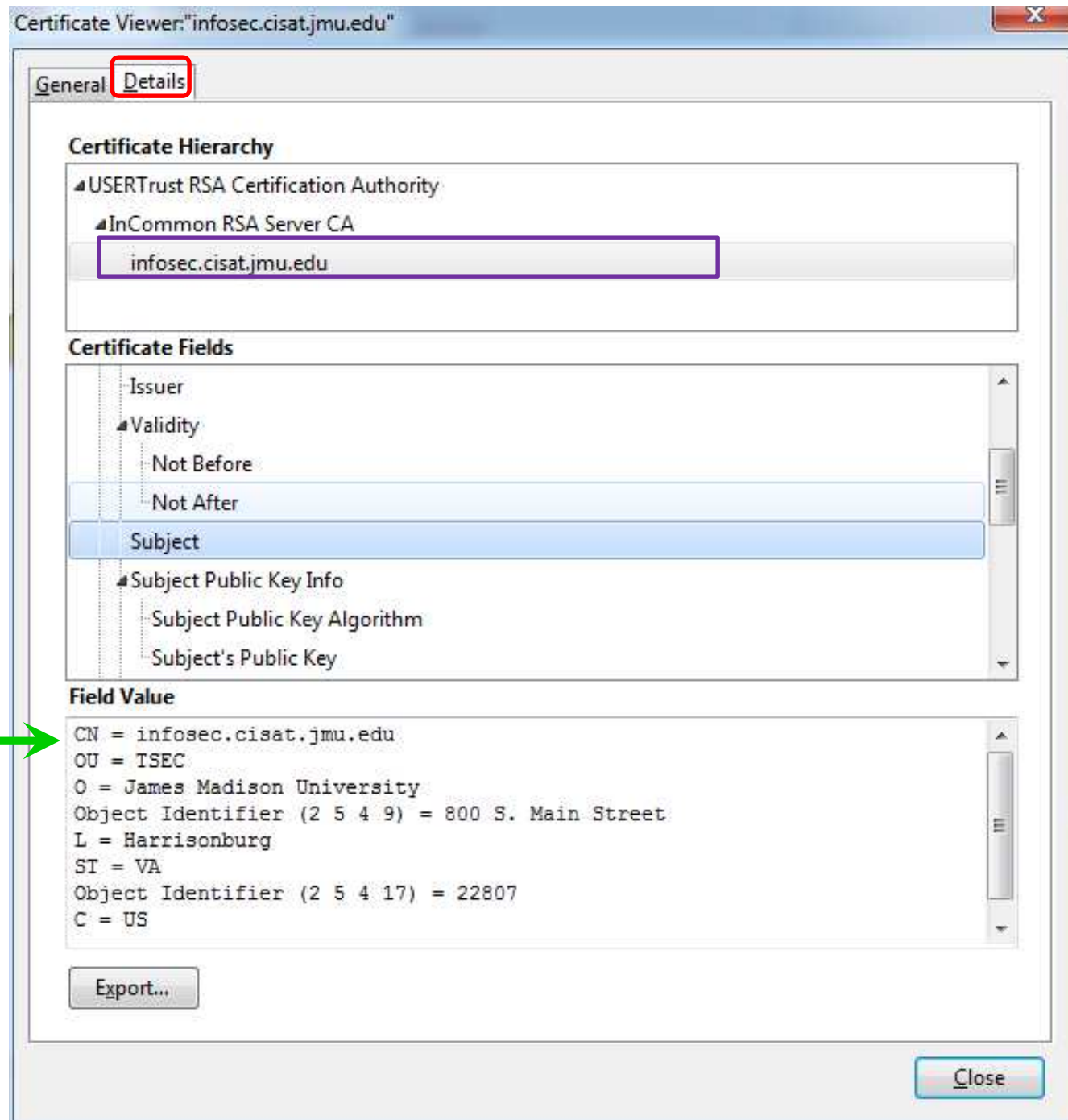
If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

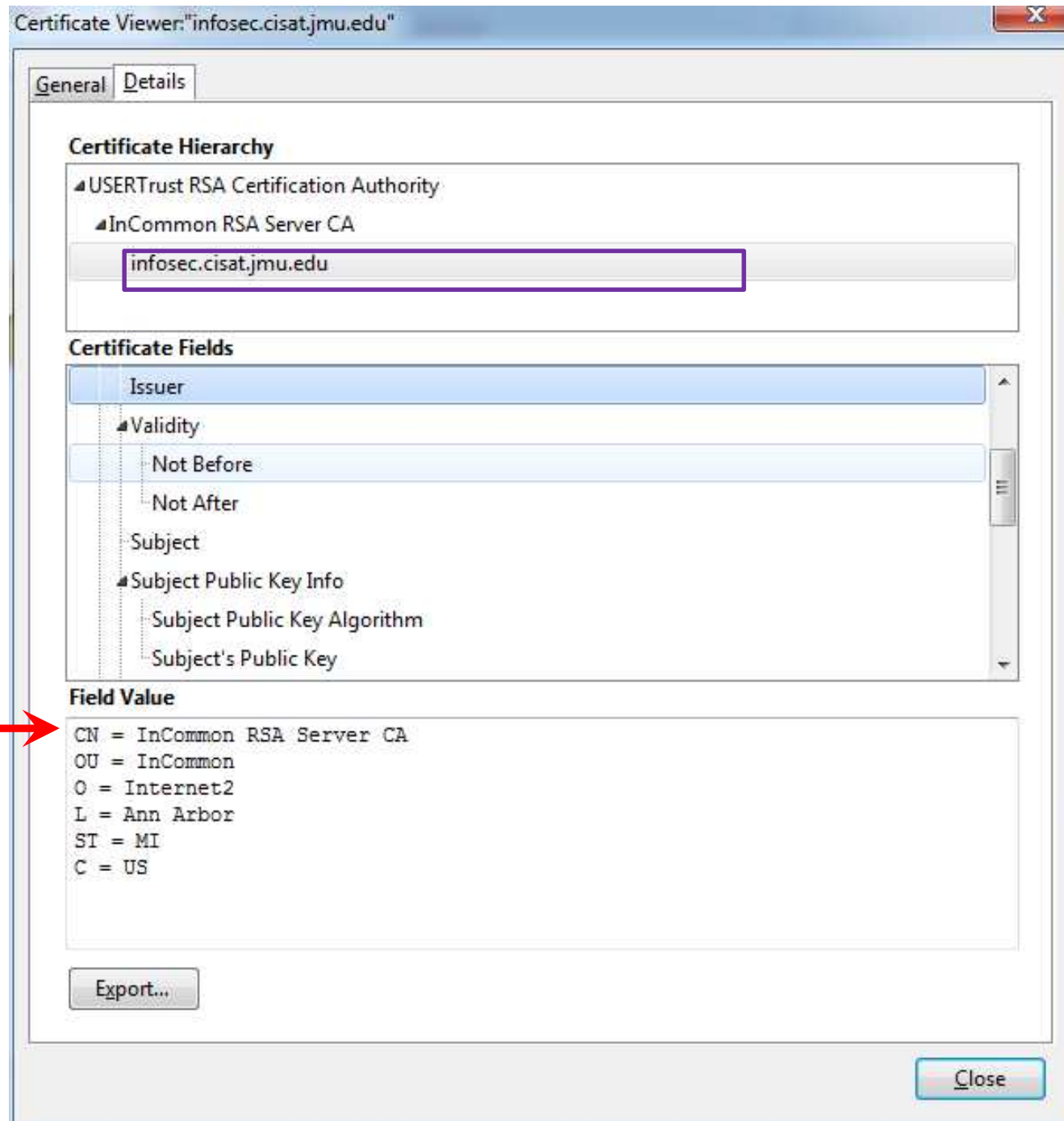
Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

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:

to identify itself with invalid information.

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

☒ Permanently store this exception

You typed in  
www.infosec.jmu.edu

But the certificate is for  
infosec.cisat.jmu.edu

File Edit View History Bookmarks Tools Help

Master's Degree in Information... x +

https://www.infosec.jmu.edu Search

JAMES MADISON UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE

# Master's Degree in COMPUTER SCIENCE

## CONCENTRATION IN INFORMATION SECURITY

Support Us | Find

SEARCH:

Home About Curriculum Our People Student Resources

### Announcements

**University Hours**  
May 11 - August 21  
8:00 a.m. - 5:00 p.m. Monday - Thursday.  
8:00 a.m. - noon on Friday.

**June 15-19**  
[GenCyber: Cyber Defense Boot Camp for High School Technology Teachers](#)

**October 14-16**  
[Grace Hopper Celebration](#)  
Registration opens on June 2

[Prerequisites for new CS Curriculum](#)

[Curriculum Change FAQs \(PDF\)](#)



One of the Original Seven National Centers of Academic Excellence in Information Assurance Education 4011, 4012, 4013, 4014, and 4015 Certified

### Welcome to the Program



working professionals program is delivered asynchronously over any location. [More >](#)

### News

[See All](#)



**[GenCyber: Cyber Defense Boot Camp for High School Technology Teachers](#)**  
March 4, 2015

**info**  
Information Security  
JAMES MADISON UNIVERSITY





# Summary

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