Internet Security

Dr. Charles Severance <csev@umich.edu>
http://www.dr-chuck.com/
Twitter: @drchuck

https://www.coursera.org/course/insidetheinternet

coursera

Paranoia

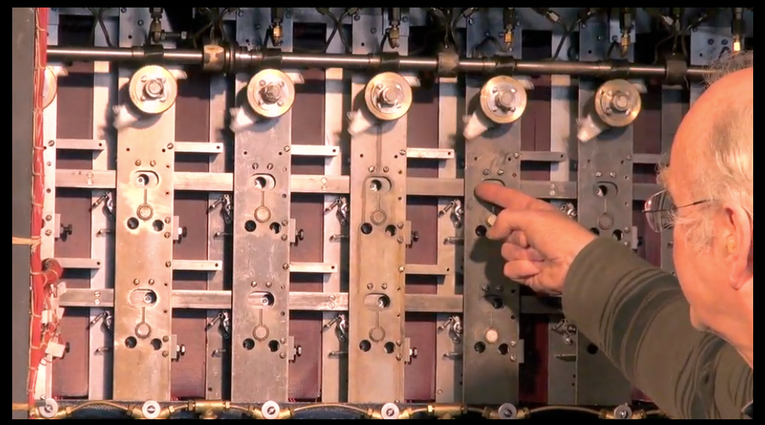
- Who is out to get you?
- If you are interesting or influential people want to get into your personal info.
- If you are normal, folks want to use your resources or take your information to make money…
- Usually no one cares… But it is safest to assume some is always trying…

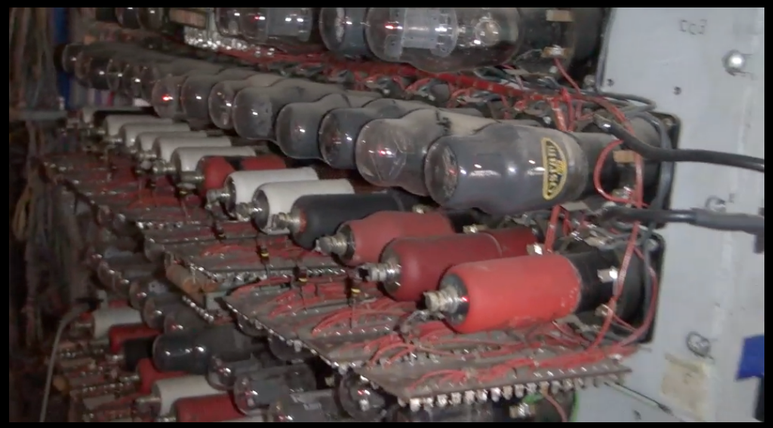
Security is always a Tradeoff

- "Perfect security" is unachievable - Must find the right tradeoff
- Security .versus. Cost
- Security .versus. Convenience (See also, "profit")
- "More" is not always better – vendors of products will try to convince you that you *cannot live* without their particular gadget

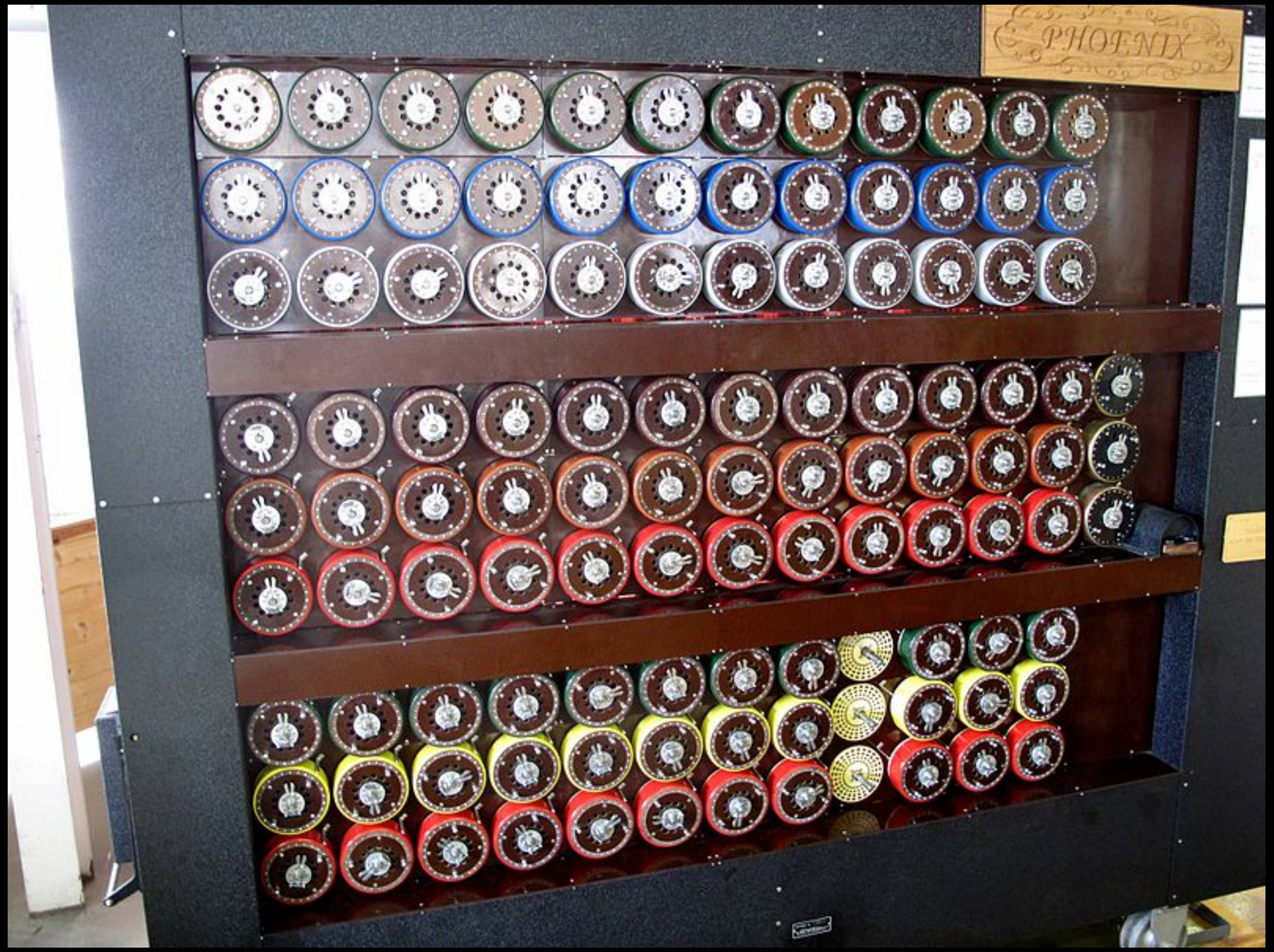
Alan Turing and Bletchley Park

- Top secret code breaking effort
- 10,000 people at the peak (team effort)
- BOMBE: Mechanical Computer
- Colossus: Electronic Computer



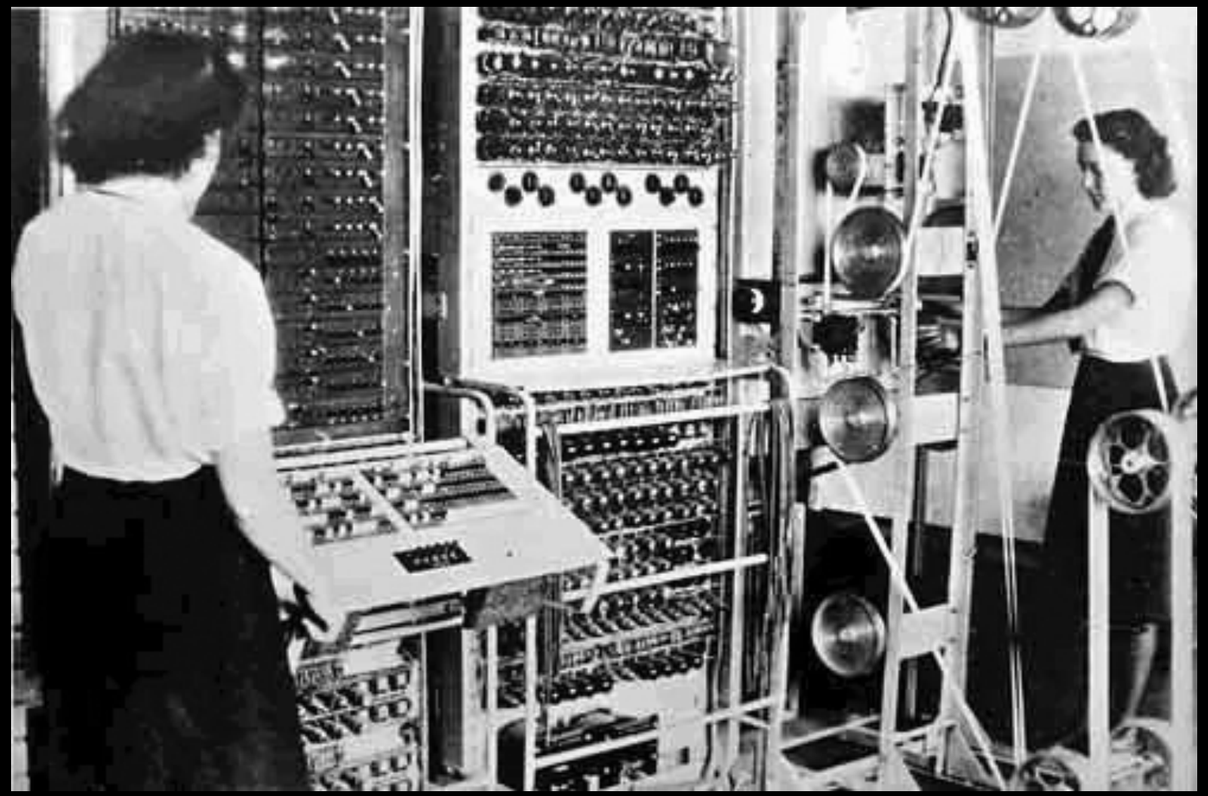


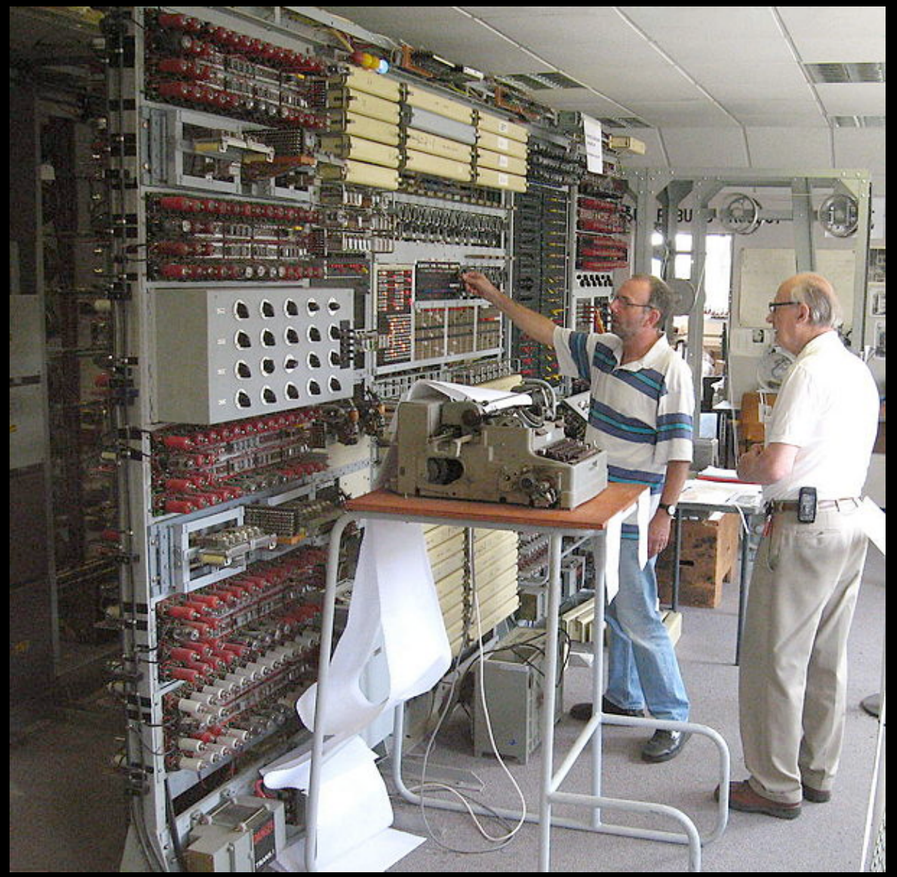
http://www.youtube.com/watch?v=5nK_ft0Lf1s



http://en.wikipedia.org/wiki/Bombe

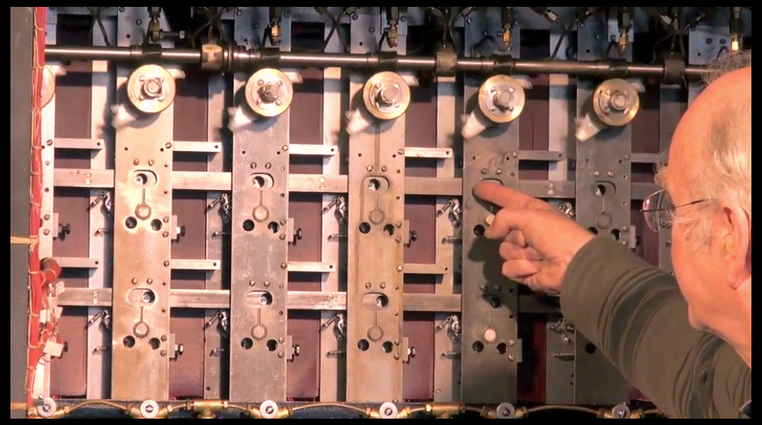
http://en.wikipedia.org/wiki/Colossus_computer

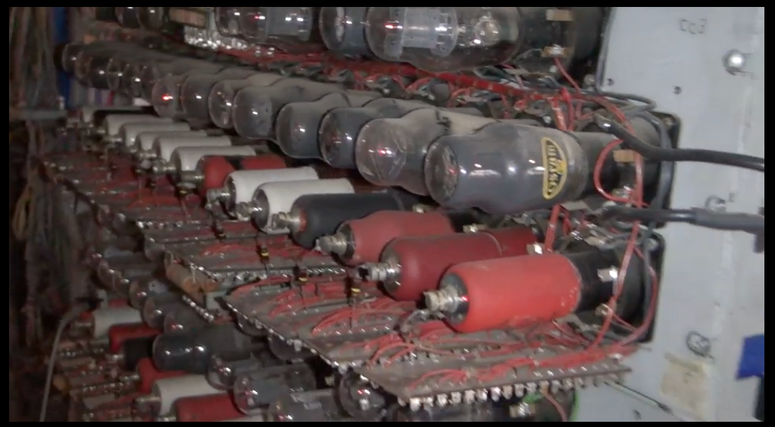




http://en.wikipedia.org/wiki/Tony_Sale


http://nmap.org/movies.html
nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: cl
Port State Service
22/tcp open ssh
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanneds
sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Resetting root password to "Z1ON0101".
System open: Access Level <9>
ssh 10.2.2.2 -l root
root@10.2.2.2's password:
ACCESS GRANTED





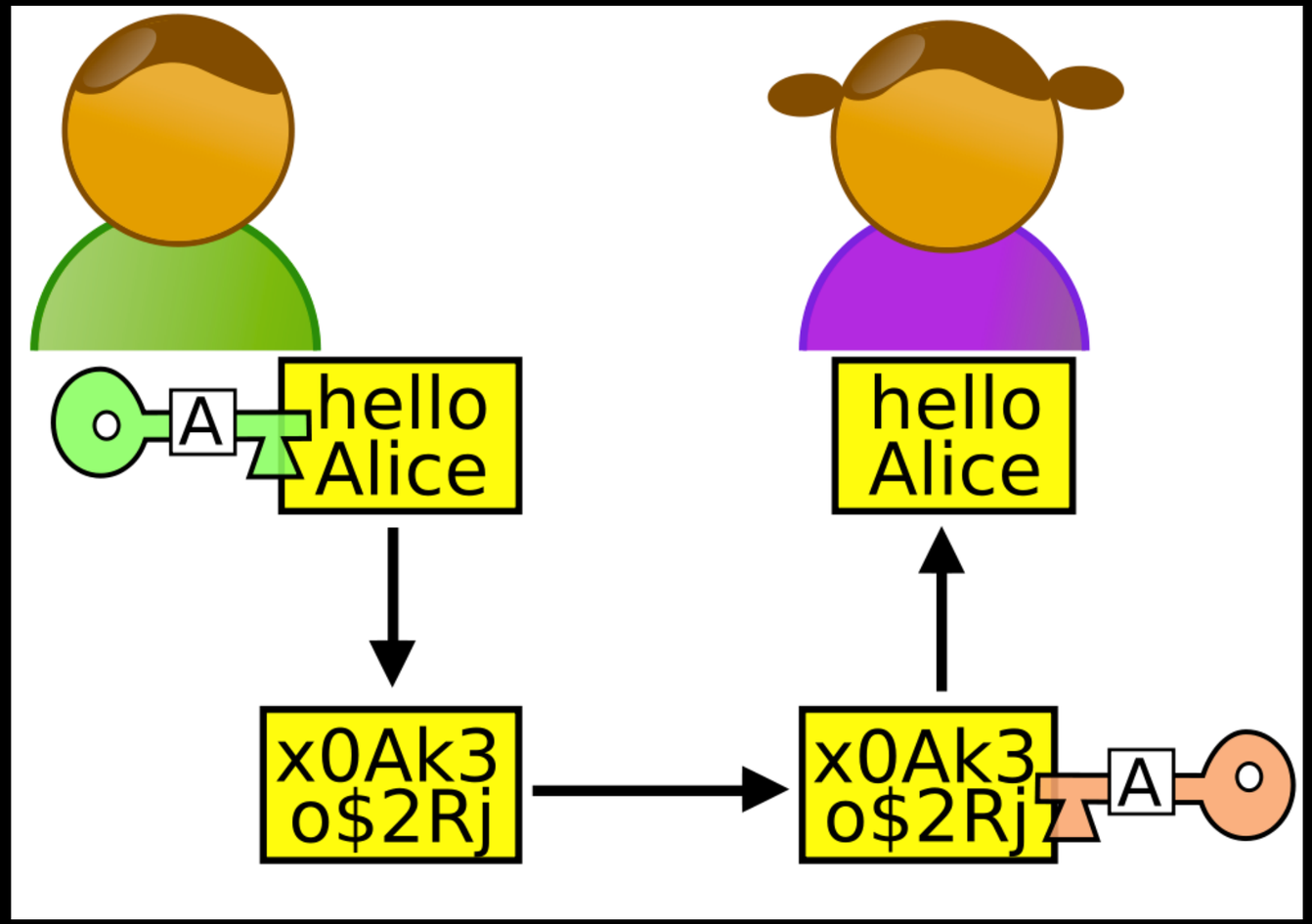
http://en.wikipedia.org/wiki/Tony_Sale

January 1931 – August 2011

http://www.youtube.com/watch?v=5nK_ft0Lf1s


"BENEDICT CUMBERBATCH IS OUTSTANDING"
RADIO TIMES
"THE BEST BRITISH FILM OF THE YEAR"
★★★★★
THE INDEPENDENT
"AN INSTANT CLASSIC"
★★★★★
GLAMOUR
"A SUPERB THRILLER"
★★★★
EMPIRE
★★★★ ★★★★
TIME OUT THE TIMES
THE IMITATION GAME
BENEDICT CUMBERBATCH
KEIRA KNIGHTLEY
12A
BASED ON THE INCREDIBLE TRUE STORY
/ImitationGameUK
IN CINEMAS NOVEMBER 14

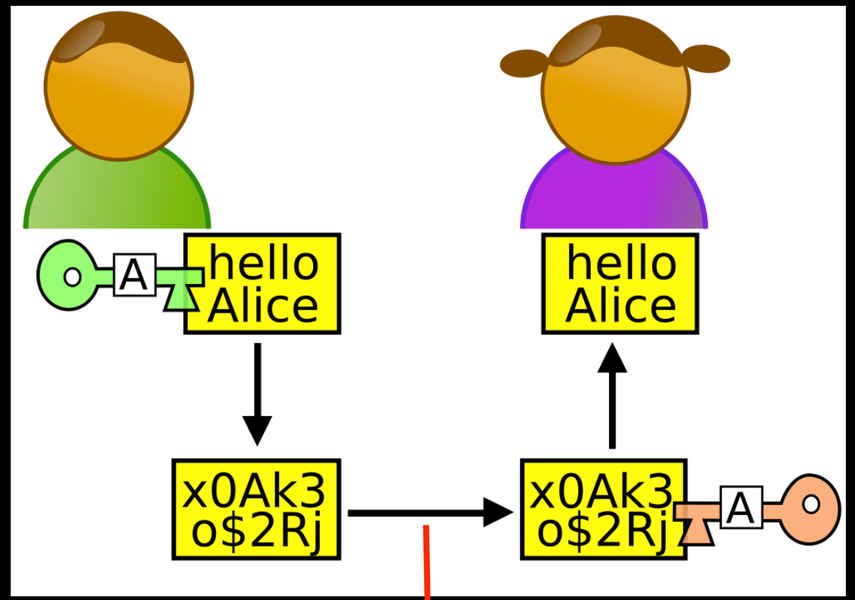
Lets Meet some Nice People

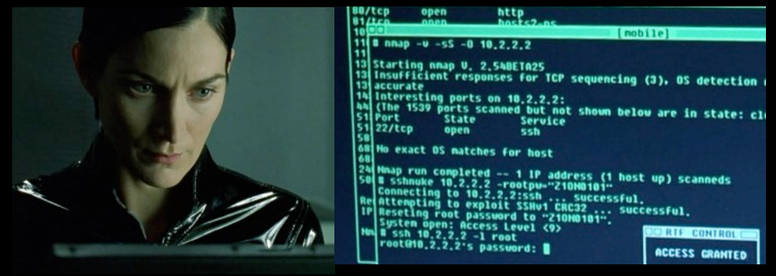


http://en.wikipedia.org/wiki/Alice_and_Bob

People With Bad Intent

- *Carol, Carlos or Charlie, as a third participant in communications.*
- *Chuck, as a third participant usually of malicious intent*
- *Dan or Dave, a fourth participant,*
- *Eve, an eavesdropper, is usually a passive attacker. While she can listen in on messages between Alice and Bob, she cannot modify them.*
- .....





http://en.wikipedia.org/wiki/Alice_and_Bob

Terminology

- Confidentiality
  - Prevent unauthorized viewing of private information
- Integrity
  - Information is from who you think it is from and has not been modified since it was sent

Ensuring Confidentiality
Encryption and Decryption

Terminology

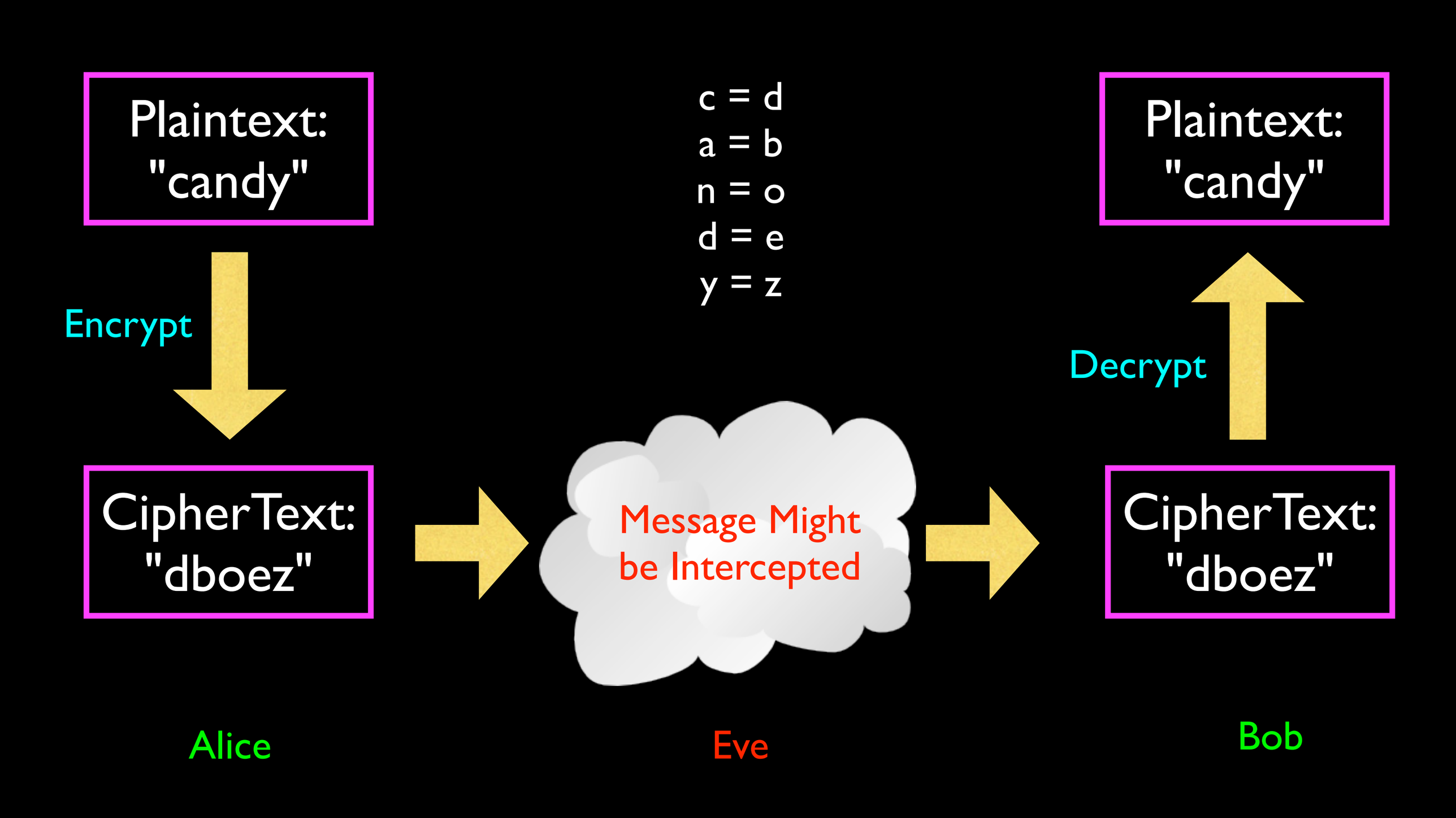
- Plaintext is a message that will be put into secret form.
- Ciphertext is a transformed version of plaintext that is unintelligible to anyone without the means to decrypt

Terminology

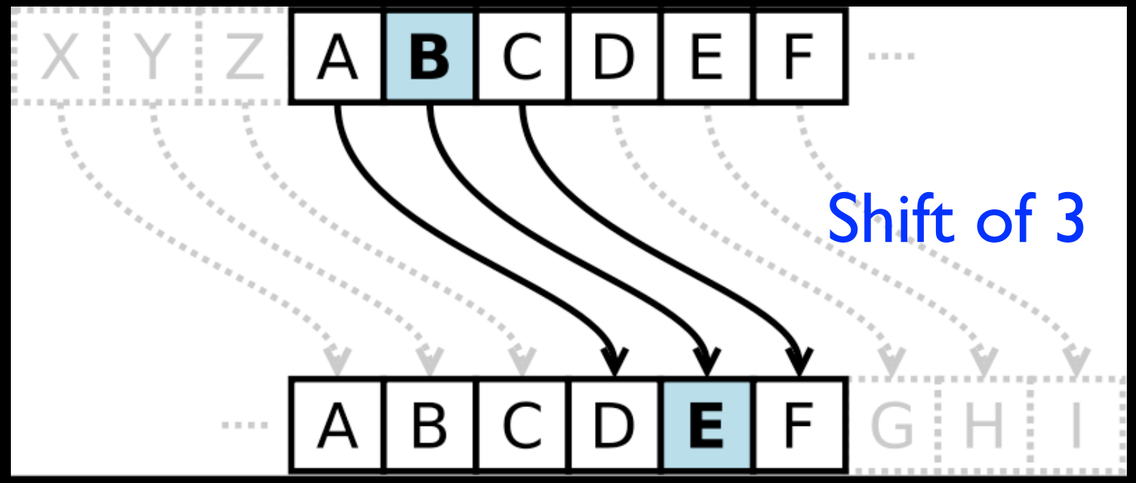
- The transformation of plaintext to ciphertext is referred to as encryption.
- Returning the ciphertext back to plaintext is referred to as decryption.
- The strength of a cryptosystem is determined by the encryption and decryption techniques and the length of the key.

Two Kinds of Systems

- Two basic types of cryptosystems exist, secret-key and public-key.
- In a secret-key scheme, the key used for encryption must be the same key used for decryption. Also called symmetric-key cryptosystem.
- Secret-key cryptosystems have the problem of secure key distribution to all parties using the cryptosystem.


Plaintext:
"candy"
c = d
a = b
n = o
d = e
y = z
Plaintext:
"candy"
Encrypt
Decrypt
CipherText:
"dboez"
Message Might
be Intercepted
CipherText:
"dboez"
Alice
Eve
Bob

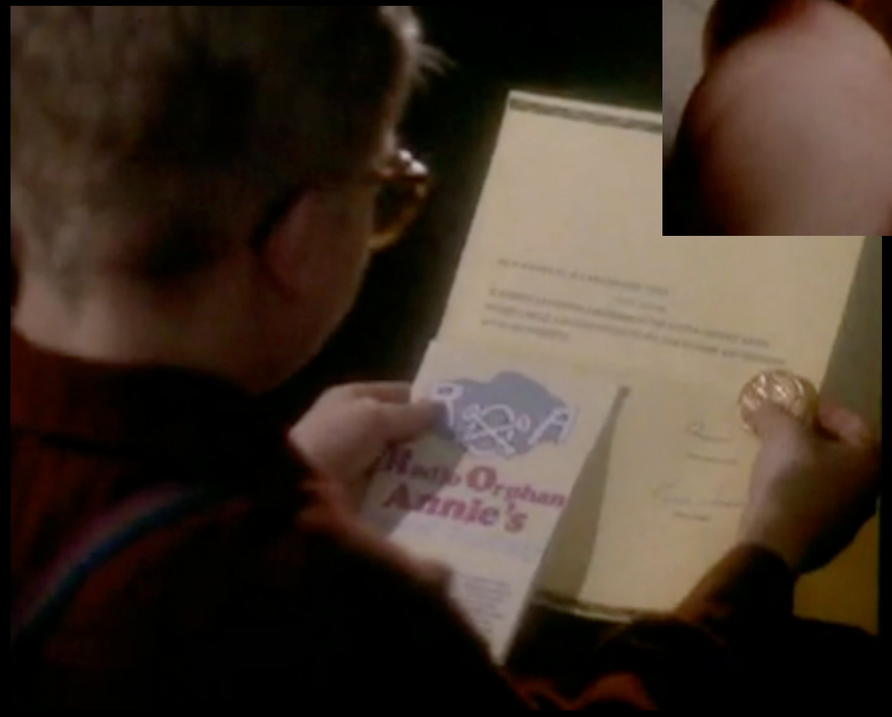
Caesar Cipher



Caesar cipher is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.

http://en.wikipedia.org/wiki/Caesar_cipher

Secret Decoder Ring



http://www.youtube.com/watch?v=zdA__2tKoIU

Secret Decoder Ring - Shift Number

```
PP:  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
01:  B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
02:  C D E F G H I J K L M N O P Q R S T U V W X Y Z A B

08:  I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
09:  J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
10:  K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
11:  L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
12:  M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
13:  N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
14:  O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
```

http://www.dr-chuck.com/Secret-Decoder.pdf

Break the Code I

CipherText:
"upbtu"

For each number 1..26, see if when you decrypt the message using that shift, it makes sense.

Break the Code I

CipherText:
"upbtu"

Plaintext:
"toast"

```
00:  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
01:  B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
```

A shift of 1

Break the Code II

Uryyb, zl anzr vf Puhpx naq V arrq zbarl naq n wrg.

Break the Code II

Uryyb, zl anzr vf Puhpx naq V arrq zbarl naq n wrg.

Hello, my name is Chuck and I need money and a jet.

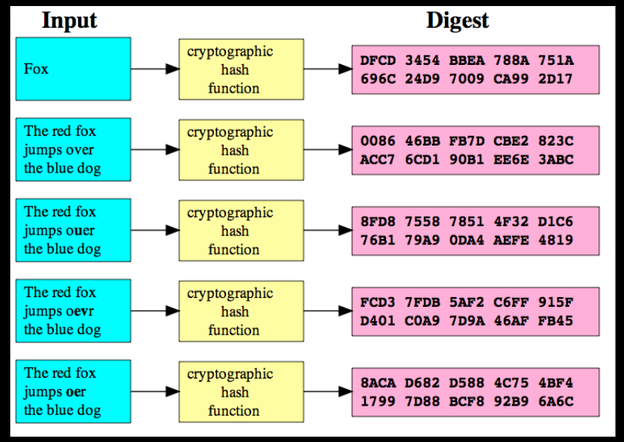
www.rot13.com

Cryptographic Hashes
Integrity

Terminology

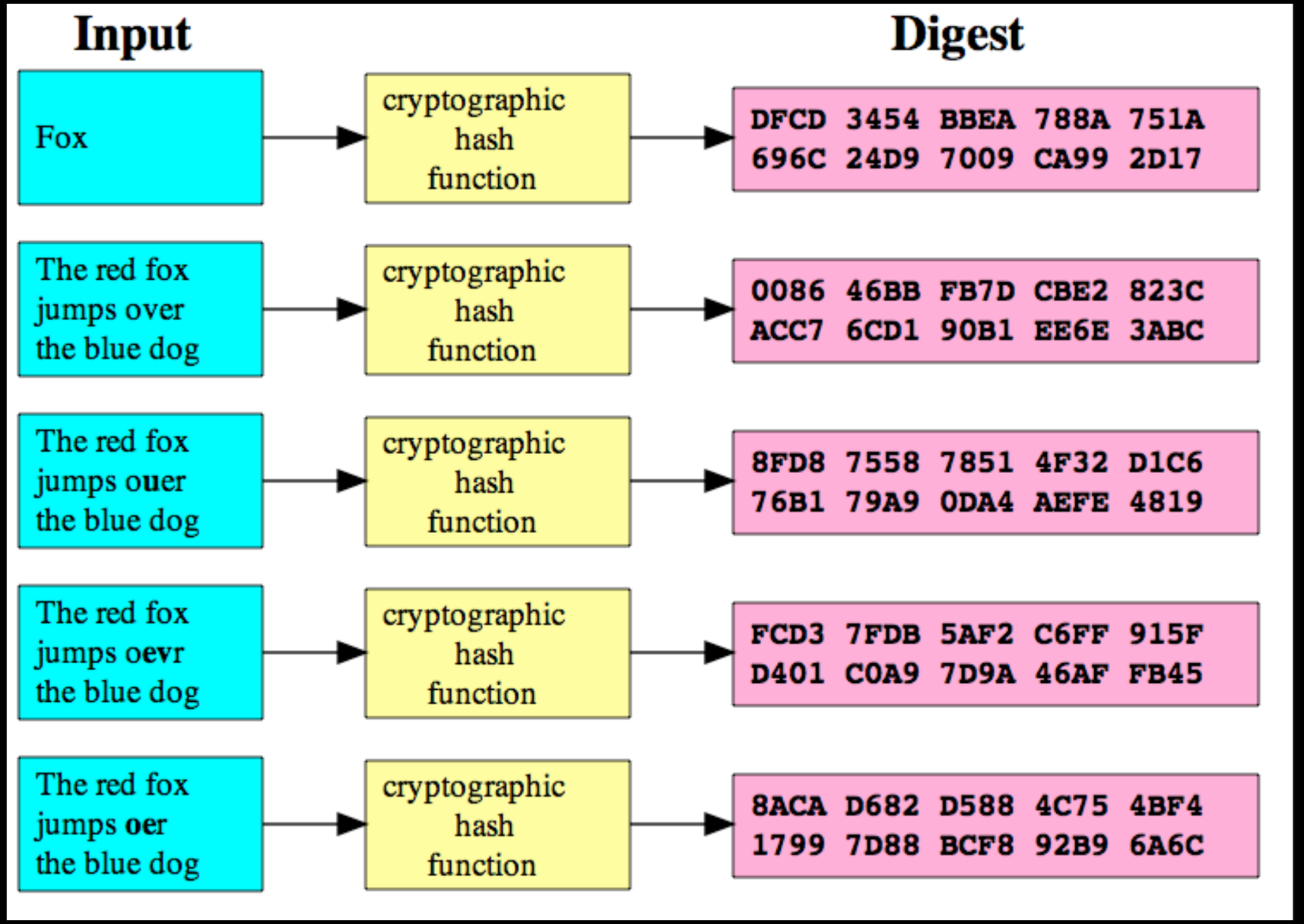
- Confidentiality
  - Prevent unauthorized viewing of private information
- Integrity
  - Information is from who you think it is from and has not been modified since it was sent

Cryptographic Hash

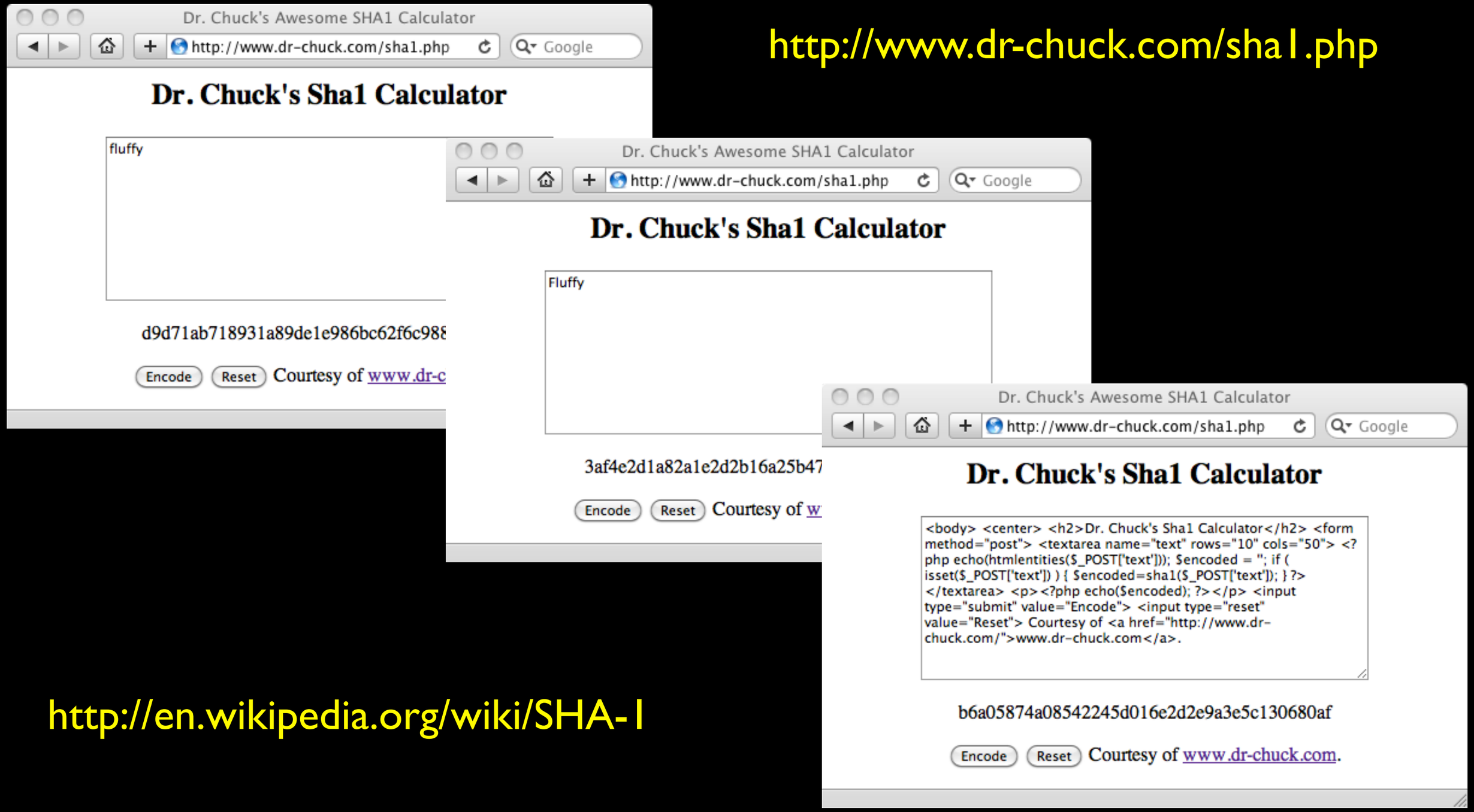


A cryptographic hash function is a function that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message," and the hash value is sometimes called the message digest or simply digest.

http://en.wikipedia.org/wiki/Cryptographic_hash_function



http://en.wikipedia.org/wiki/Cryptographic_hash_function



http://www.dr-chuck.com/sha1.php

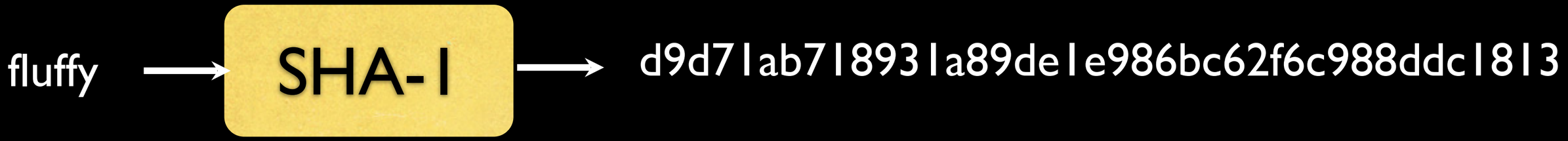
http://en.wikipedia.org/wiki/SHA-1

Hashes for Passwords

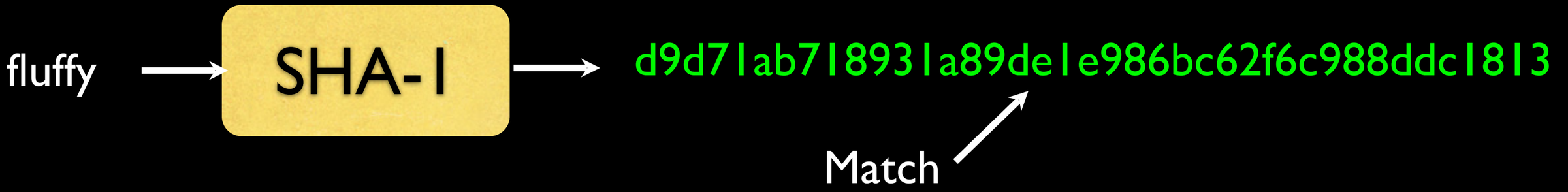
- As a general rule, systems do not store your password in plain text their databases in case they 'lose' their data
- When you set the password, they compute a hash and store the hash
- When you try to log in they compute the hash of what you type as a password and if it matches what they have stored - they let you in.
- This is why a respectable system will never send your PW to you - they can only reset it!

Setting a new password

Store the 'hashed password' in the database.



Log in attempt



http://www.dr-chuck.com/sha1.php

Digital Signatures
Message Integrity

Message Integrity

- When you get a message from someone, did that message really come from who you think it came from?
- Was the message altered while in transit or is the copy you received the same as the copy that was sent?

You

"Eat More
Ovaltine
-- Annie"

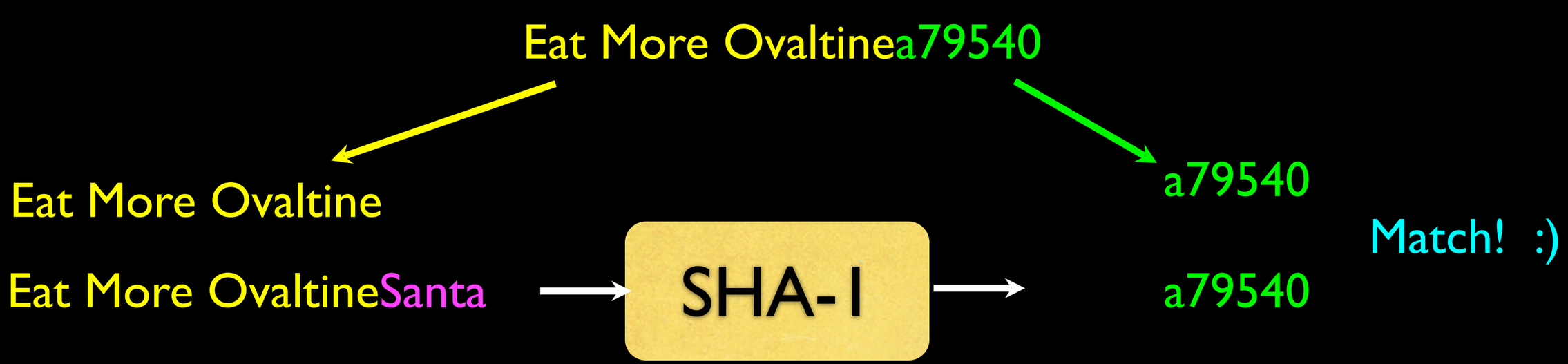
How might we be very sure this message really came from Annie and it was not altered enroute?

Simple Message Signing

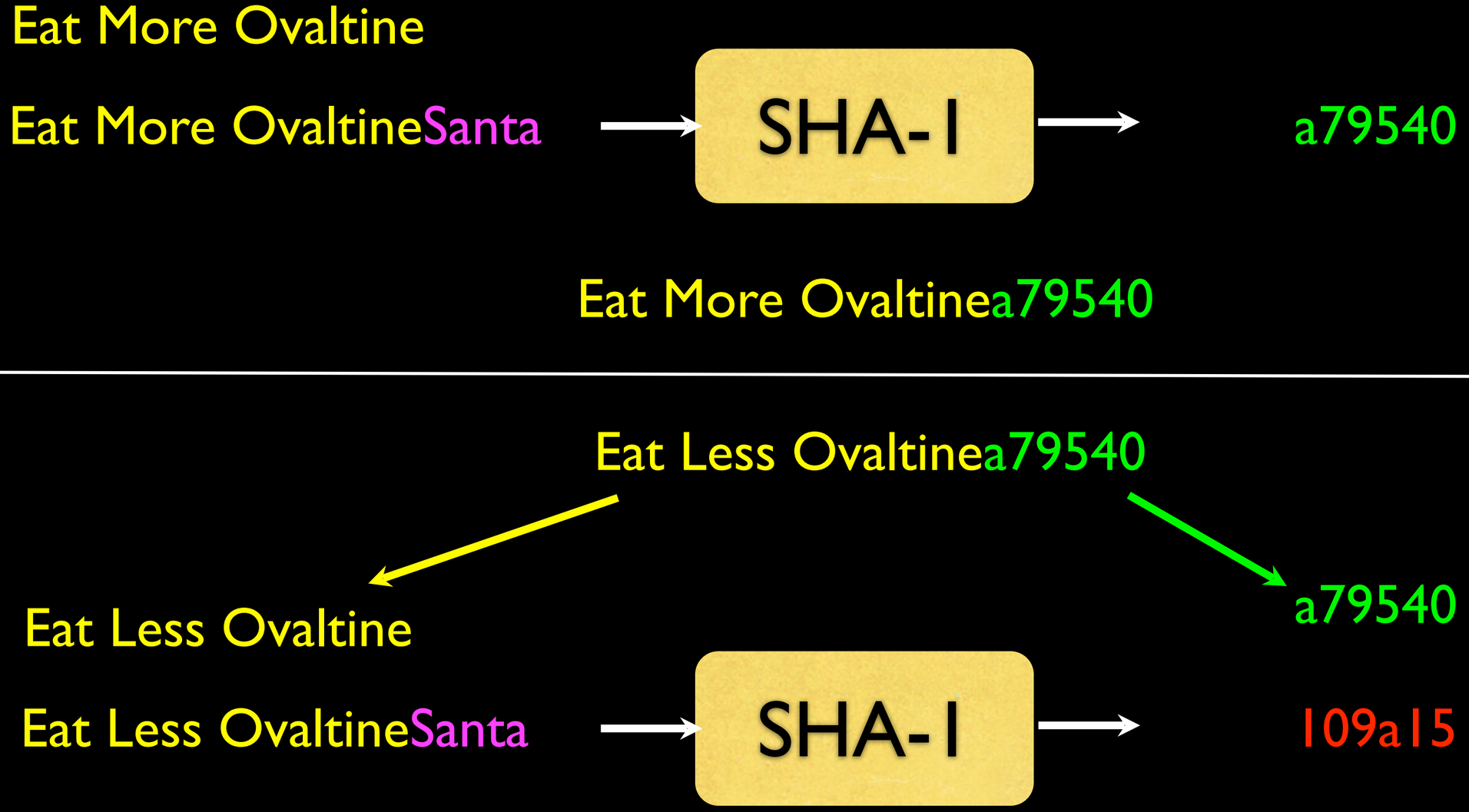
- Shared secret transported securely 'out of band'
- Before sending the message, concatenate the secret to the message
- Compute the SHA digest of the message+secret
- Send message + digest across insecure transport

Receiving a Signed Message

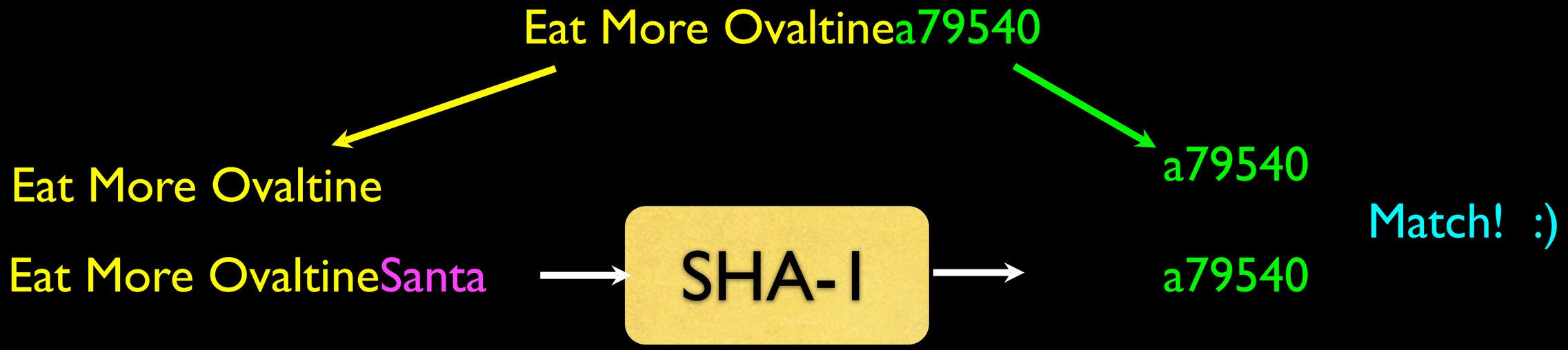
- Receive message + digest from insecure transport
- Remove digest and add secret
- Compute SHA digest for message + secret
- Compare the computed digest to the received digest



http://www.dr-chuck.com/sha1.php



http://www.dr-chuck.com/sha1.php

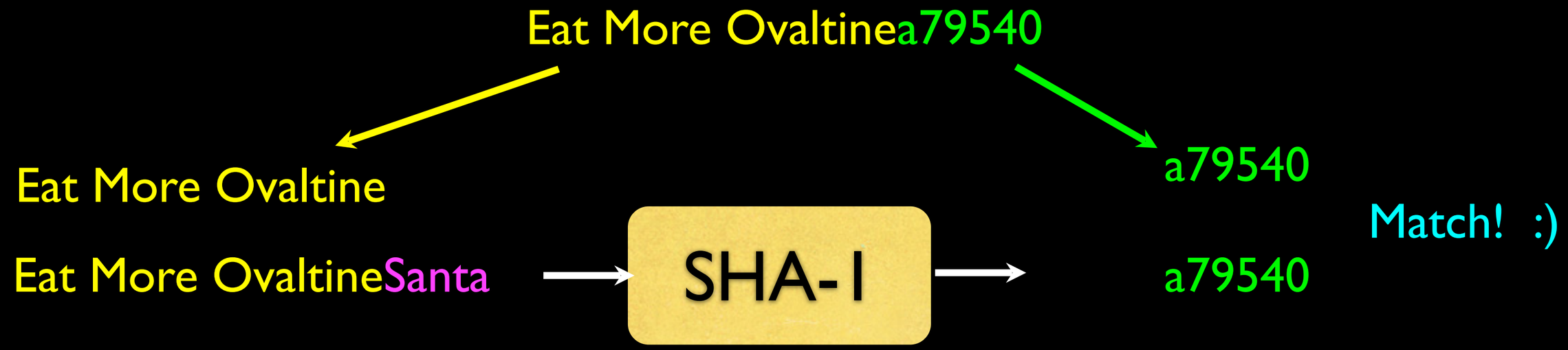


Free Cookies84d211

Free Candy26497c

Which of these is real and which is fake?

http://www.dr-chuck.com/sha1.php

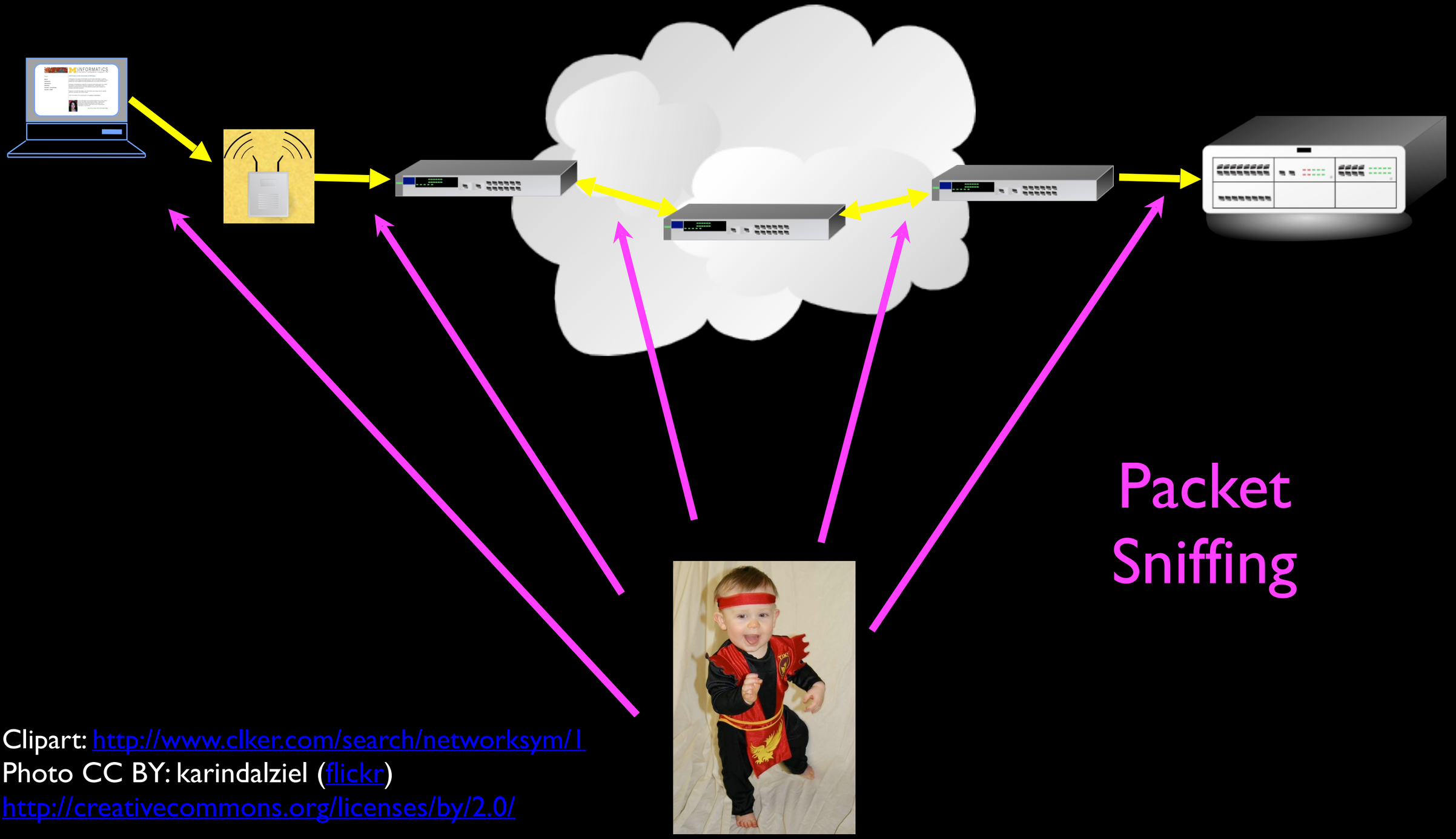


Free Cookies84d211	Free CookiesSanta	c14d5d	✗
Free Candy26497c	Free CandySanta	26497c	✓

http://www.dr-chuck.com/sha1.php

Security for TCP

http://en.wikipedia.org/wiki/Secure_Sockets_Layer

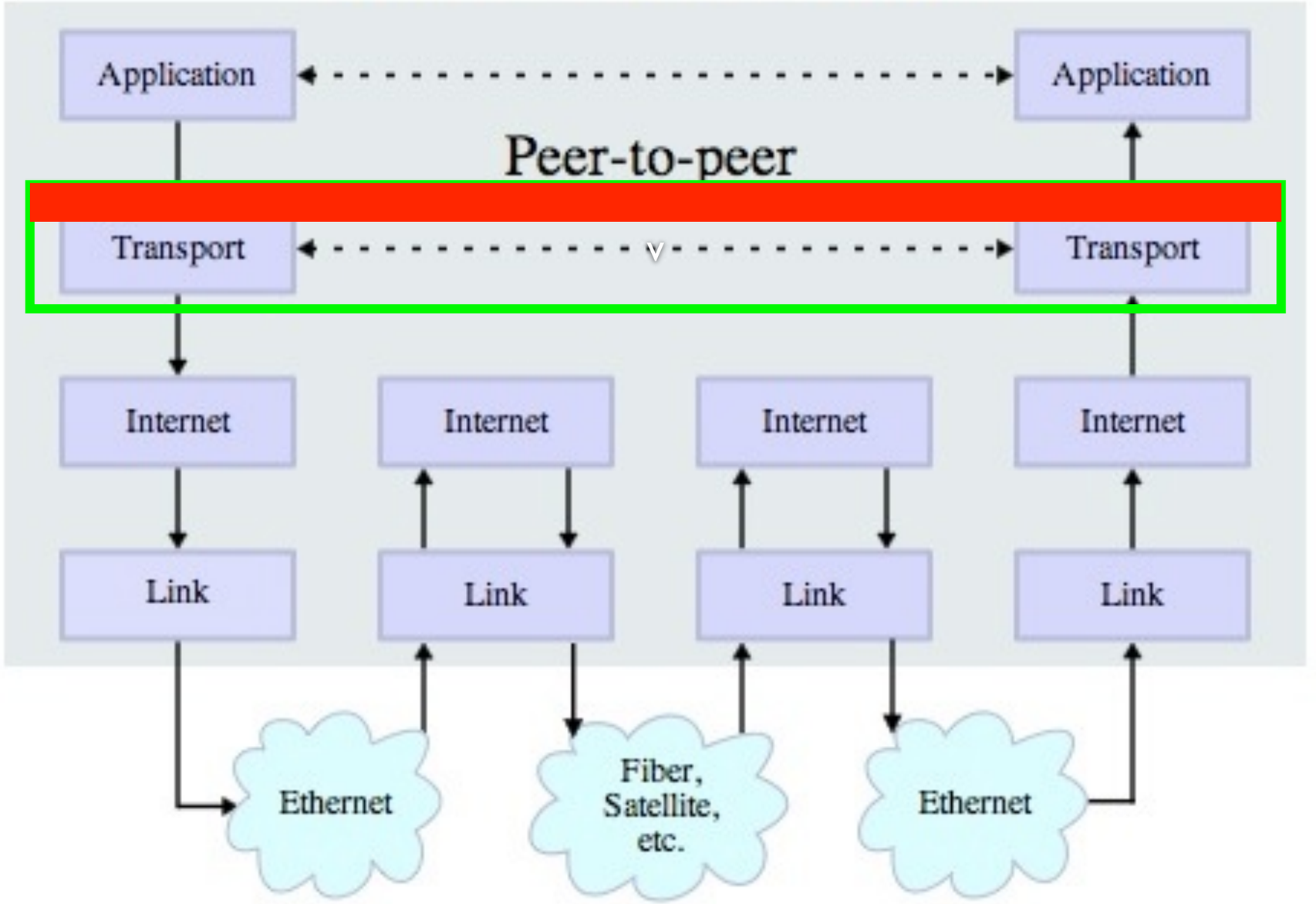


Clipart: http://www.clker.com/search/networksym/1
Photo CC BY: karindalziel (flickr)
http://creativecommons.org/licenses/by/2.0/

Transport Layer Security (TLS)

- Used to be called "Secure Sockets Layer" (SSL)
- Can view it as an extra layer "between" TCP and the application layer
- It is very difficult but not impossible to break this security - normal people do not have the necessary compute resources to break TLS
- The IP and TCP are unaware whether data has been encrypted

Stack Connections



System to System Secure TCP/IP

Web-Scale Secret Management
Public Key Encryption

Secret Key Shortcomings

- Every pair of people/systems needs a secret key
- In the Internet, key distribution cannot be via the Internet because communications are insecure until you get the key!
- For the Internet to work we need an approach where keys can cross the insecure Internet and be intercepted without compromising security

Establishing Keys at a Distance

- Proposed by Whitfield Diffie and Martin Hellman in 1976
- Public-key cryptosystems rely on two keys which are mathematically related to one another. Also called asymmetric-key cryptosystem.
- One key is called the public key and is to be openly revealed to all interested parties.
- The second key is called the private key and must be kept secret.

http://en.wikipedia.org/wiki/Public-key_cryptography

http://en.wikipedia.org/wiki/Ralph_Merkle

http://en.wikipedia.org/wiki/Martin_Hellman

http://en.wikipedia.org/wiki/Whitfield_Diffie

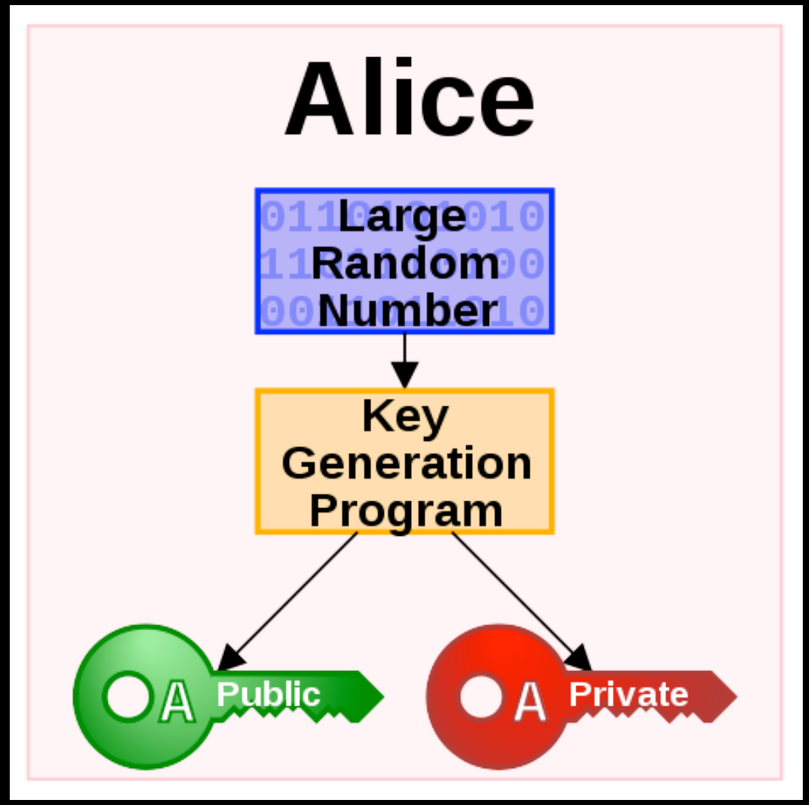
https://www.youtube.com/watch?v=ROCray7RTqM

Public Key

- A message encrypted with one of the keys can only be decrypted with the other key.
- It is computationally infeasible to recover one key from the other
- Public-key cryptosystems solve the problem of secure key distribution because the public key can be openly revealed to anyone without weakening the cryptosystem.

Generating Public/Private Pairs

- Choose two large* random prime numbers
- Multiply them
- Compute public and private keys from that very large number



*The definition of "large" keeps getting bigger as computers get faster

Public Key Math (light)

- Some functions are easy in "one direction", but in the other, not so much!
  Example: What are the factors of 55,124,159?

Public Key Math (light)

- What are the factors of 55,124,159 (a nearly prime number)
- What do you multiply 7919 by to get 55,124,159?
- If you know that one of the factors is 7919, it's also easy to find 6961!

US Patent 4,200,700 (Sep 6, 1977)

RSA Encryption

- Implementation of secure channel based on public / private keys
- Ron Rivest, Adi Shamir and Leonard Adleman

US Patent 4,405,829 (Dec 14, 1977)

http://people.csail.mit.edu/rivest/photos/Len-Adi-Ron.jpg

RSA Math (Light)

- Prime numbers: 3 * 11 = 33
- Public key: (33,7) (7 is computed from 3 and 11)
- Private key: 3
- Encrypt the letter f=6 (6**7) % 33 = 30 (sent)
- Decrypt received text: (30**3) % 33 = 6 (f)

http://www.youtube.com/watch?v=M7kEpw1tn50
http://en.wikipedia.org/wiki/Fermat's_little_theorem
http://sergematovic.tripod.com/rsa1.html

You

https

Amazon.com

Plaintext:
"Visa928"

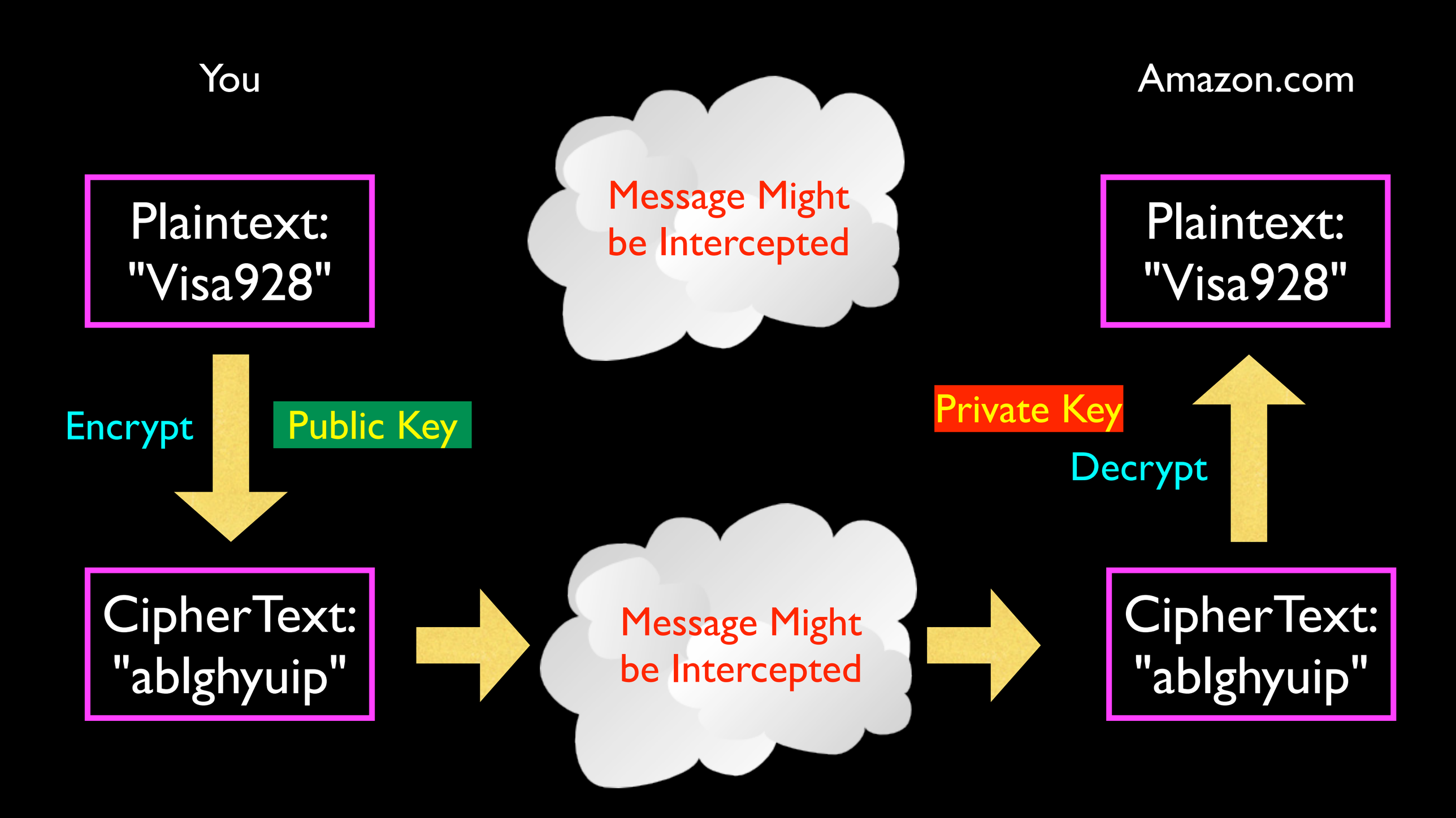
You

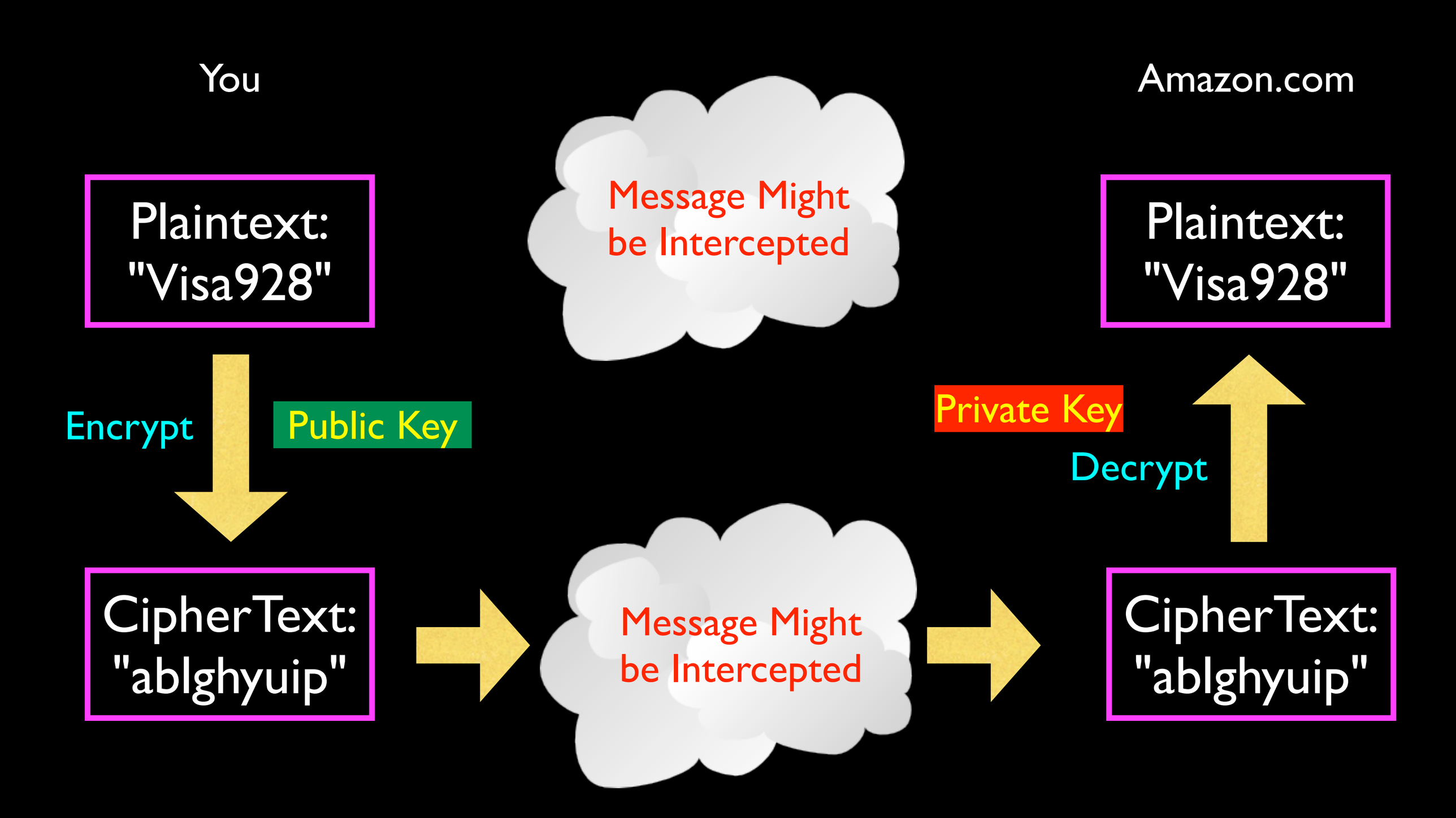
Amazon.com

Plaintext:
"Visa928"

Public Key

Private Key


You
Amazon.com
Plaintext:
"Visa928"
Message Might
be Intercepted
Plaintext:
"Visa928"
Encrypt
Public Key
Private Key
Decrypt
CipherText:
"ablghyuip"
Message Might
be Intercepted
CipherText:
"ablghyuip"


You
Amazon.com
Plaintext:
"Visa928"
Message Might
be Intercepted
Plaintext:
"Visa928"
Encrypt
Public Key
Private Key
Decrypt
CipherText:
"ablghyuip"
Message Might
be Intercepted
CipherText:
"ablghyuip"

Certificate Authorities
Integrity

Announcements | Internet History, Technology, and Security

https class.coursera.org/insidetheinternet-002/class/index

Reader

Announcements | Internet History, Technology, and Security

coursera

Charles Severance

UNIVERSITY OF MICHIGAN

- Syllabus
- Video Lectures
- Quizzes (Assignments)
- Discussion Forums
- Resources Wiki (Editable)
- Feedback Survey
- Peer Graded Essays (Extra Credit)
- Demographic Survey

Safari is using an encrypted connection to class.coursera.org.

Encryption with a digital certificate keeps information private as it's sent to or from the https website class.coursera.org.

Go Daddy Class 2 Certification Authority

Go Daddy Secure Certification Authority

*.coursera.org

***.coursera.org**

Issued by: Go Daddy Secure Certification Authority

Expires: Wednesday, January 4, 2017 8:34:00 PM Eastern Standard Time

This certificate is valid

▶ Trust

▶ Details

?

Hide Certificate

OK

than once and still keep the class in the few hours per week range.

Fri 12 Apr 2013 5:28 AM PDT -0700

Week 6 and Office Hours in Philadelphia, PA

coming Deadlines

izzes

Quiz

9 PM PDT -0700

signments

Credit Assignment 2

mission)

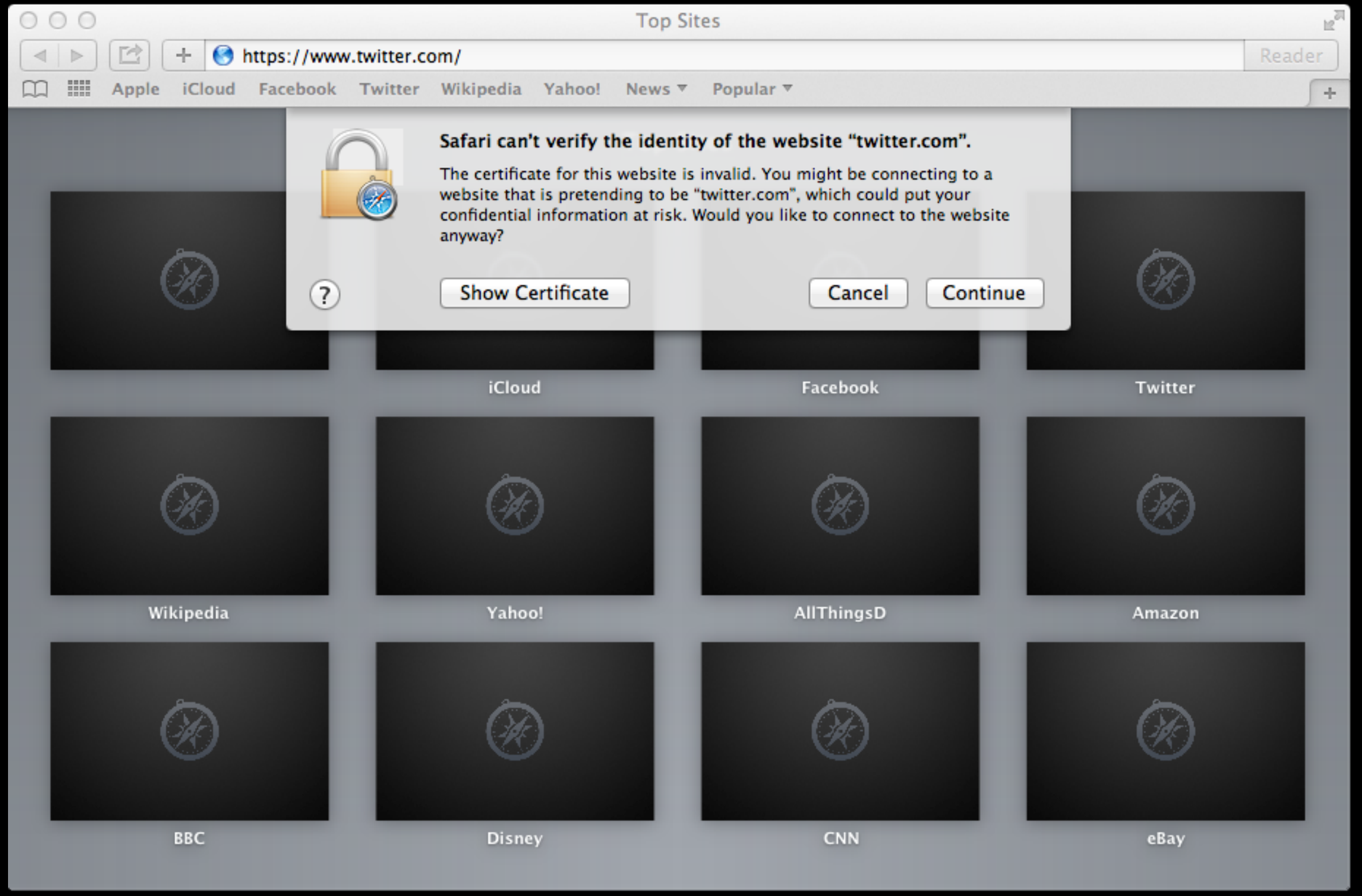
22 Apr 2013 10:36 PM PDT -0700

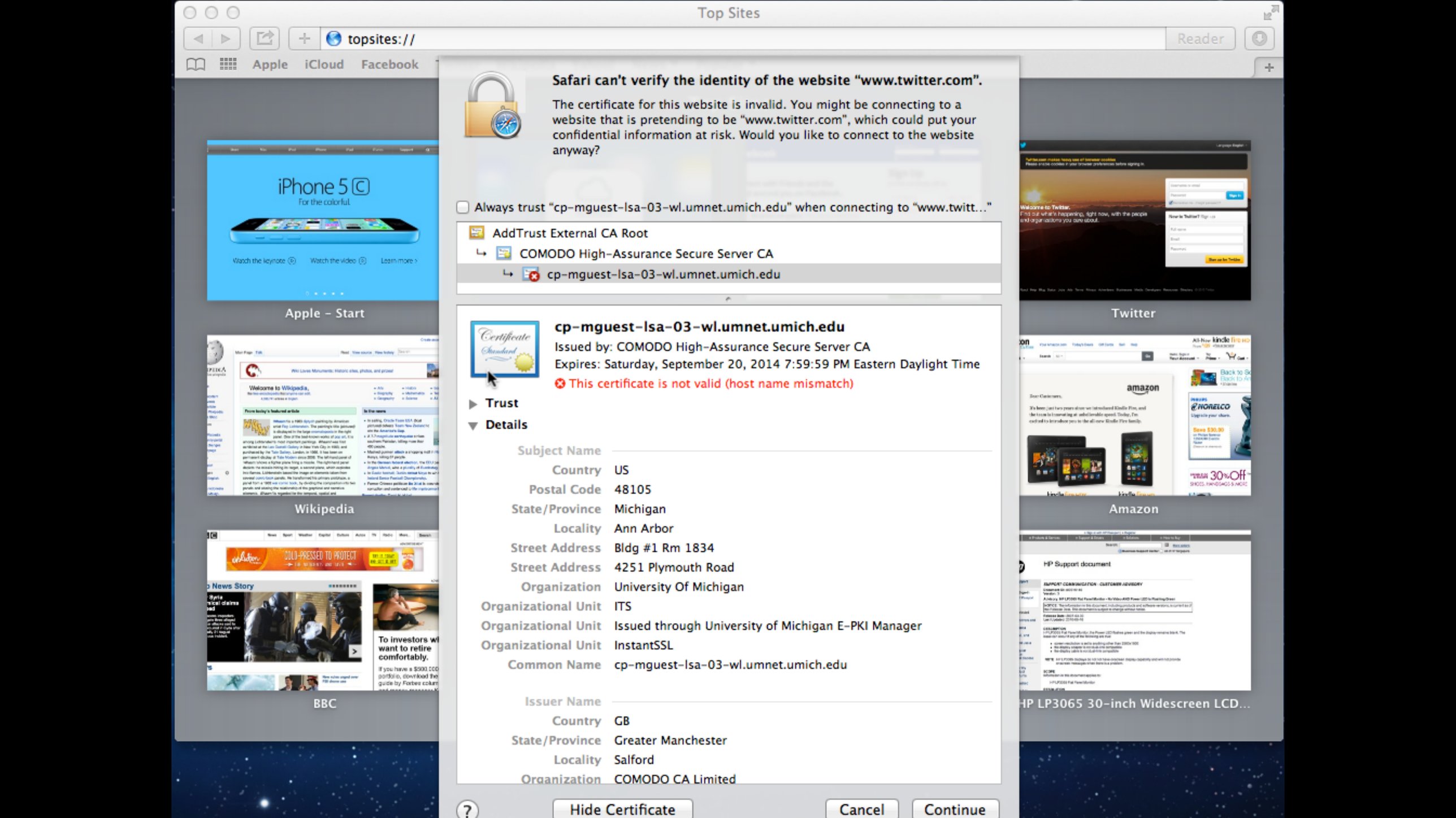
Deadlines calendar

New Lectures

Application Layer (25:13)

Van Jacobson - Content Centered Networking (10:00)


Top Sites
https://www.twitter.com/
Reader
Apple
iCloud
Facebook
Twitter
Wikipedia
Yahoo!
News
Popular
Safari can't verify the identity of the website "twitter.com".
The certificate for this website is invalid. You might be connecting to a website that is pretending to be "twitter.com", which could put your confidential information at risk. Would you like to connect to the website anyway?
Show Certificate
Cancel
Continue
iCloud
Facebook
Twitter
Wikipedia
Yahoo!
AllThingsD
Amazon
BBC
Disney
CNN
eBay


Top Sites
topsites://
Reader
Apple
iCloud
Facebook
Safari can't verify the identity of the website "www.twitter.com".
The certificate for this website is invalid. You might be connecting to a website that is pretending to be "www.twitter.com", which could put your confidential information at risk. Would you like to connect to the website anyway?
Always trust "cp-mguest-lsa-03-wl.umnet.umich.edu" when connecting to "www.twitt..."
AddTrust External CA Root
COMODO High-Assurance Secure Server CA
cp-mguest-lsa-03-wl.umnet.umich.edu
cp-mguest-lsa-03-wl.umnet.umich.edu
Issued by: COMODO High-Assurance Secure Server CA
Expires: Saturday, September 20, 2014 7:59:59 PM Eastern Daylight Time
This certificate is not valid (host name mismatch)
Trust
Details
Subject Name
Country US
Postal Code 48105
State/Province Michigan
Locality Ann Arbor
Street Address Bldg #1 Rm 1834
Street Address 4251 Plymouth Road
Organization University Of Michigan
Organizational Unit ITS
Organizational Unit Issued through University of Michigan E-PKI Manager
Organizational Unit InstantSSL
Common Name cp-mguest-lsa-03-wl.umnet.umich.edu
Issuer Name
Country GB
State/Province Greater Manchester
Locality Salford
Organization COMODO CA Limited
Hide Certificate
Cancel
Continue
Apple - Start
Twitter
Wikipedia
Amazon
BBC
HP LP3065 30-inch Widescreen LCD...

Public-Key Issues

- Public-key cryptosystems have the problem of securely associating a public key with an individual
- I am about to type in my credit card and send it - am I being Phished?
- The remote server sent me a public key.
- Should I use it? Is this really Amazon's public key?

http://en.wikipedia.org/wiki/Phishing

Digital Certificates

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

http://en.wikipedia.org/wiki/Public_key_certificate

Certificate Authority (CA)

A certificate authority is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. A CA is a trusted third party that is trusted by both the owner of the certificate and the party relying upon the certificate.

http://en.wikipedia.org/wiki/Certificate_authority

VeriSign Authentication Services – The leading provider of SSL. Products ...rotection, malware scan, code signing & public key infrastructure (PKI).

http://www.verisign.com/

verisign

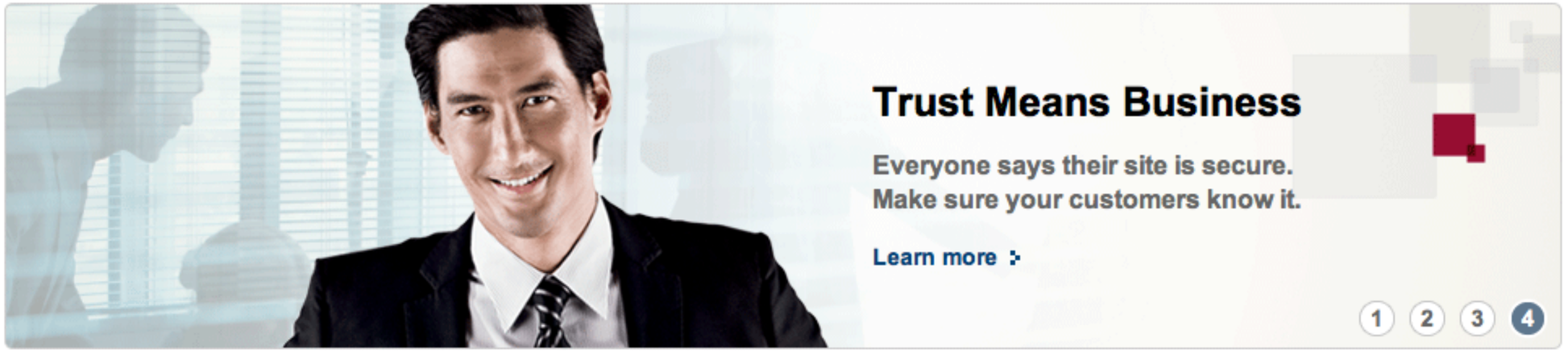
United States [change] | Contact Us

Now from Symantec. | VeriSign Authentication Services

Search

VeriSign Trusted VERIFY

Products & Services | Partners | Support | My Account



BUY SSL Certificates

BUY VeriSign Trust Seal

BUY Code Signing

TRY Free Trial NEW!

RENEW Renew SSL Certificates

SIGN IN VeriSign Trust Center

Trust from Search to Browse to Buy

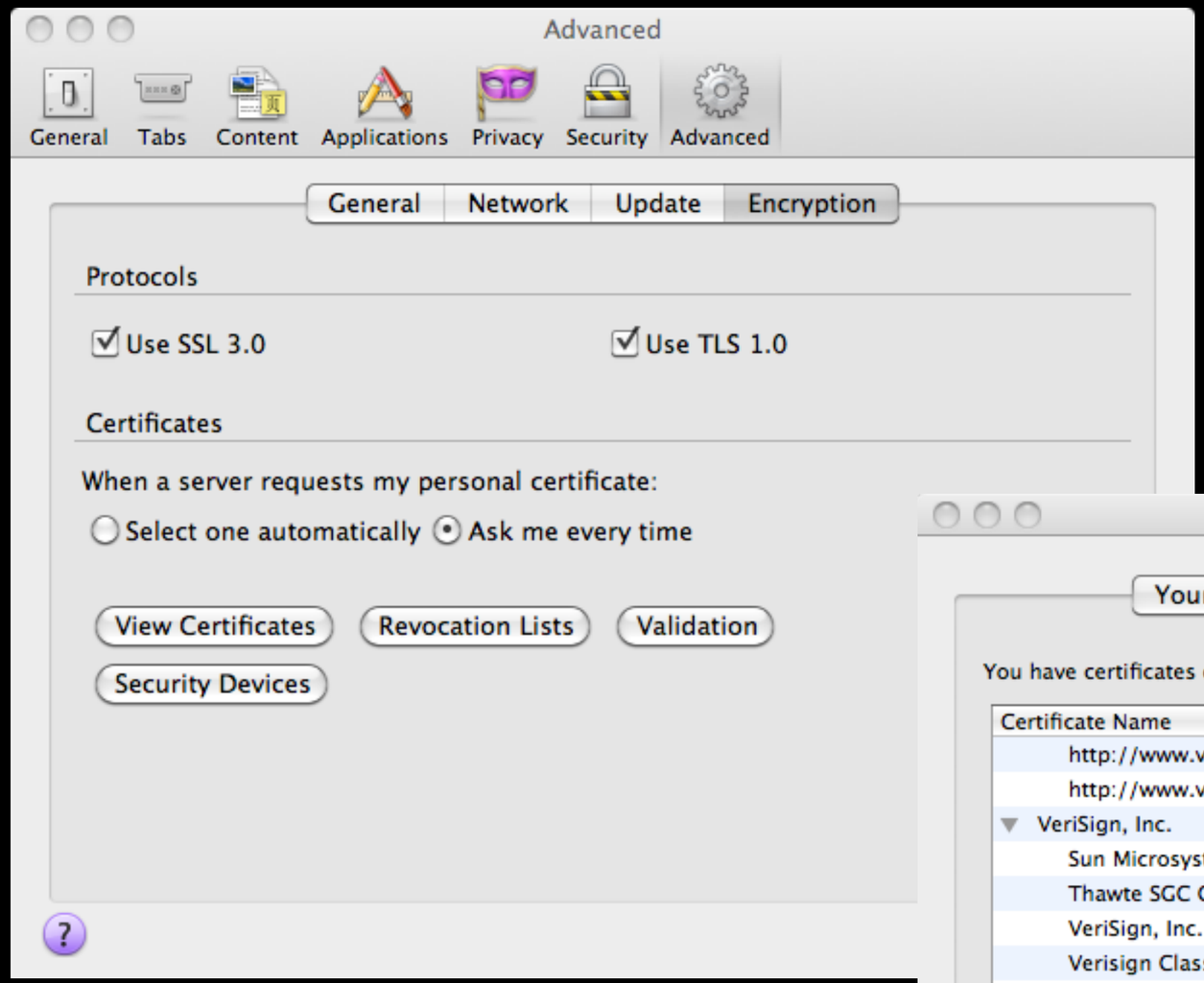
Boost your site traffic and conversions with powerful trust features. Free with every SSL Certificate.

Protect your Business from Online Threats

Find a Symantec solution to secure, backup and manage your valuable data.

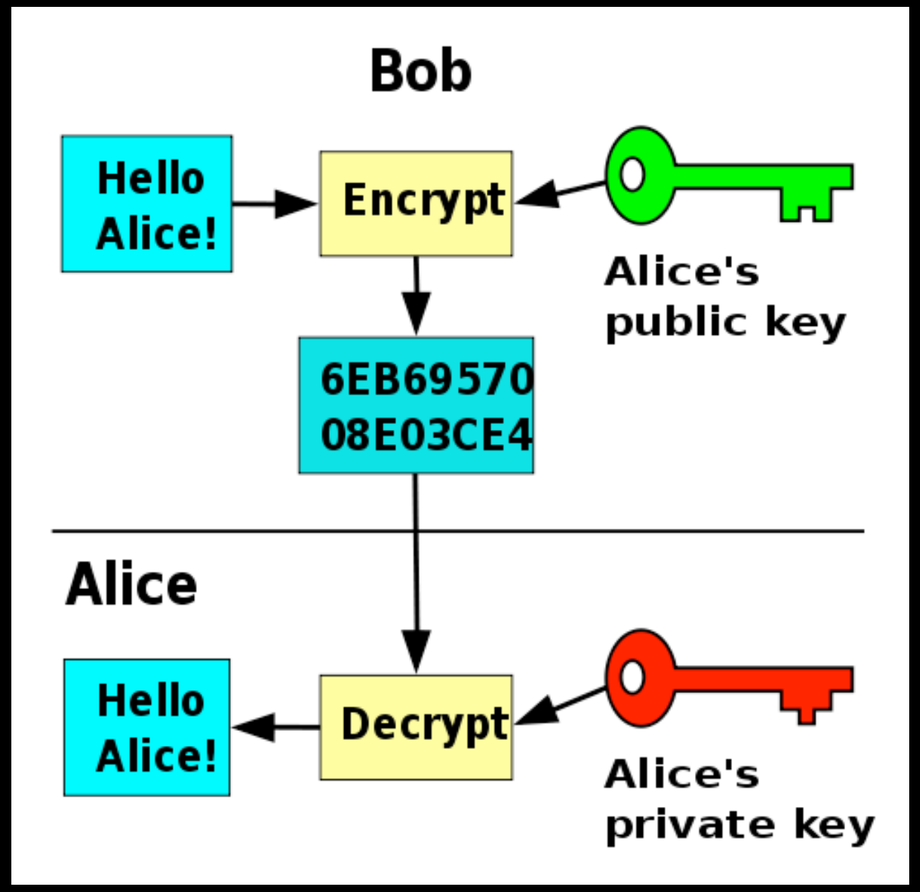
VERISIGN

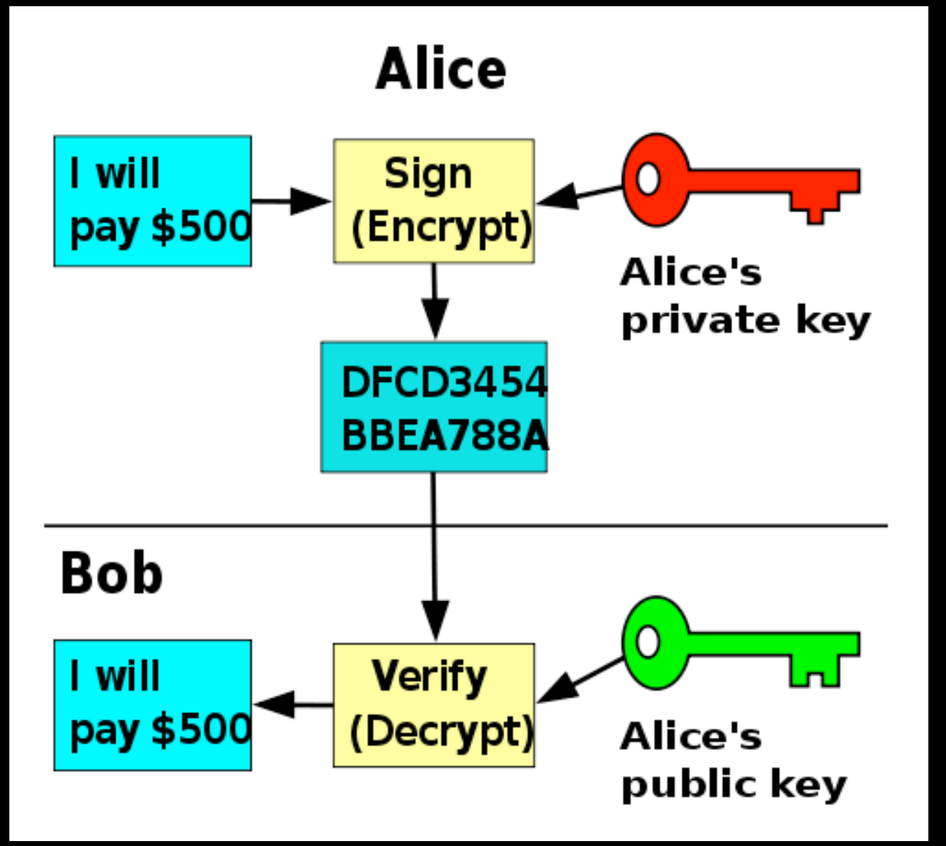
Find WhoIs, Registrar Information, Domain Name Services, Managed DNS, DDoS Protection and iDefense at



Your browser comes with certificates/public keys from some certificate authorities built in. Like Verisign.

Public/Private Keys for Signing





http://en.wikipedia.org/wiki/Public-key_cryptography

How Amazon gets a public key signed by Verisign

Verisign

Verisign Private Key

Verisign Public Key

Amazon

Your Laptop

When you bought your laptop

Verisign

Verisign Private Key

Amazon Public Key

Amazon Private Key

Verisign Public Key

Amazon

Your Laptop

Six months ago

Verisign

Verisign Private Key

Amazon Public Key

Amazon Public Key

Amazon Private Key

Verisign Public Key

Amazon

Your Laptop

Six months ago

Verisign

Verisign Private Key

Amazon Public Key

Cert: Amazon
-- Verisign

Amazon Public Key

Amazon Private Key

Verisign Public Key

Amazon

Your Laptop

Six months ago

Verisign

Verisign Private Key

Amazon Public Key

Cert: Amazon
-- Verisign

Amazon Private Key

Verisign Public Key

Amazon

Your Laptop

Six months ago

Verisign

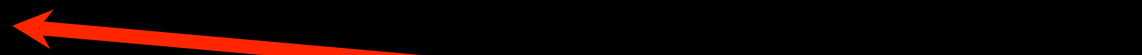
Verisign Private Key

Amazon Public Key

Cert: Amazon
-- Verisign

Amazon Private Key

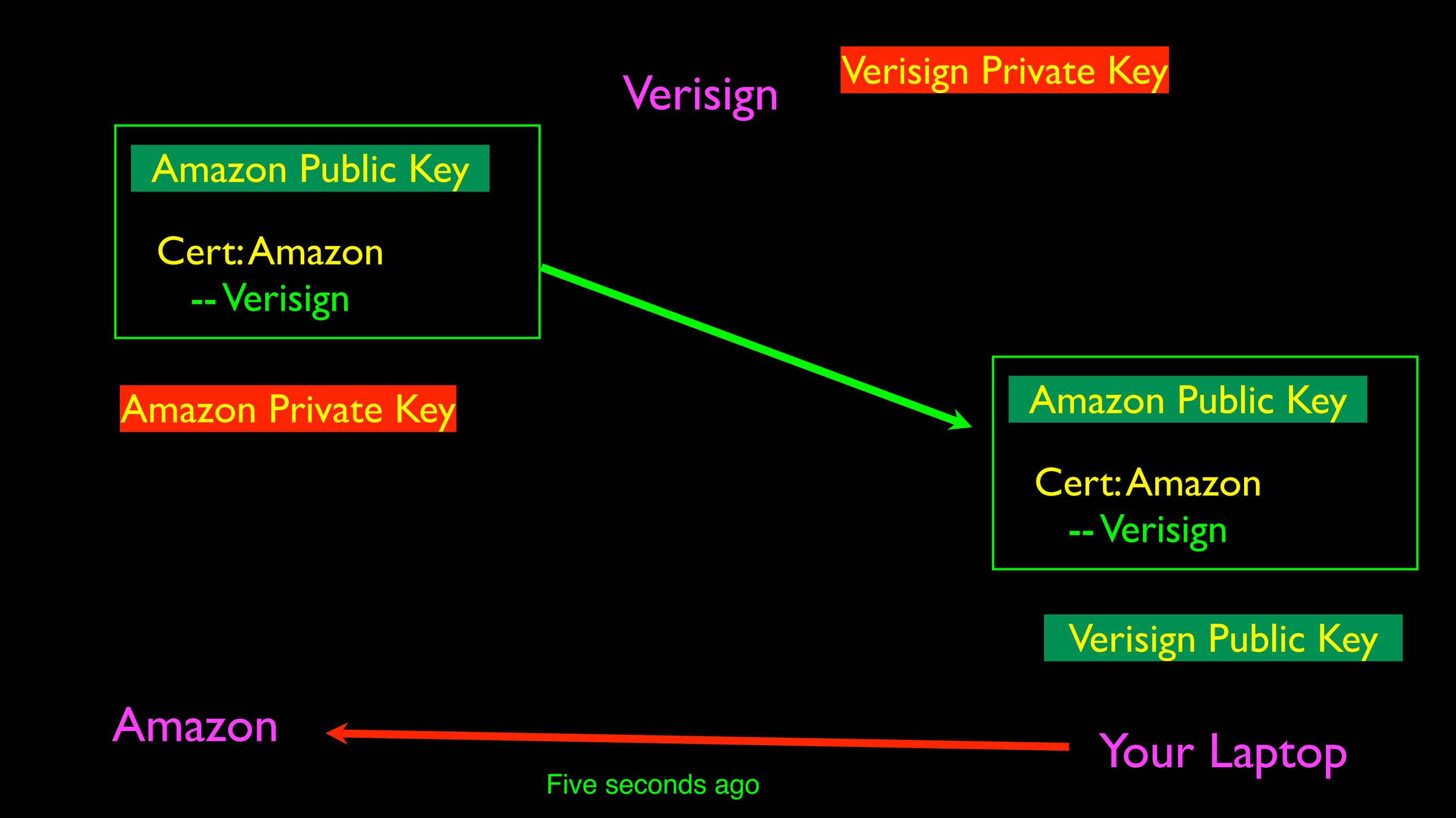
Verisign Public Key



Amazon

Your Laptop

Five seconds ago


Verisign
Verisign Private Key
Amazon Public Key
Cert: Amazon
-- Verisign
Amazon Private Key
Amazon Public Key
Cert: Amazon
-- Verisign
Verisign Public Key
Amazon
Your Laptop
Five seconds ago

Verisign

Verisign Private Key

Amazon Public Key

Cert: Amazon
-- Verisign

Amazon Private Key

Amazon Public Key

Cert: Amazon
-- Verisign

Verisign Public Key

Amazon

Your Laptop

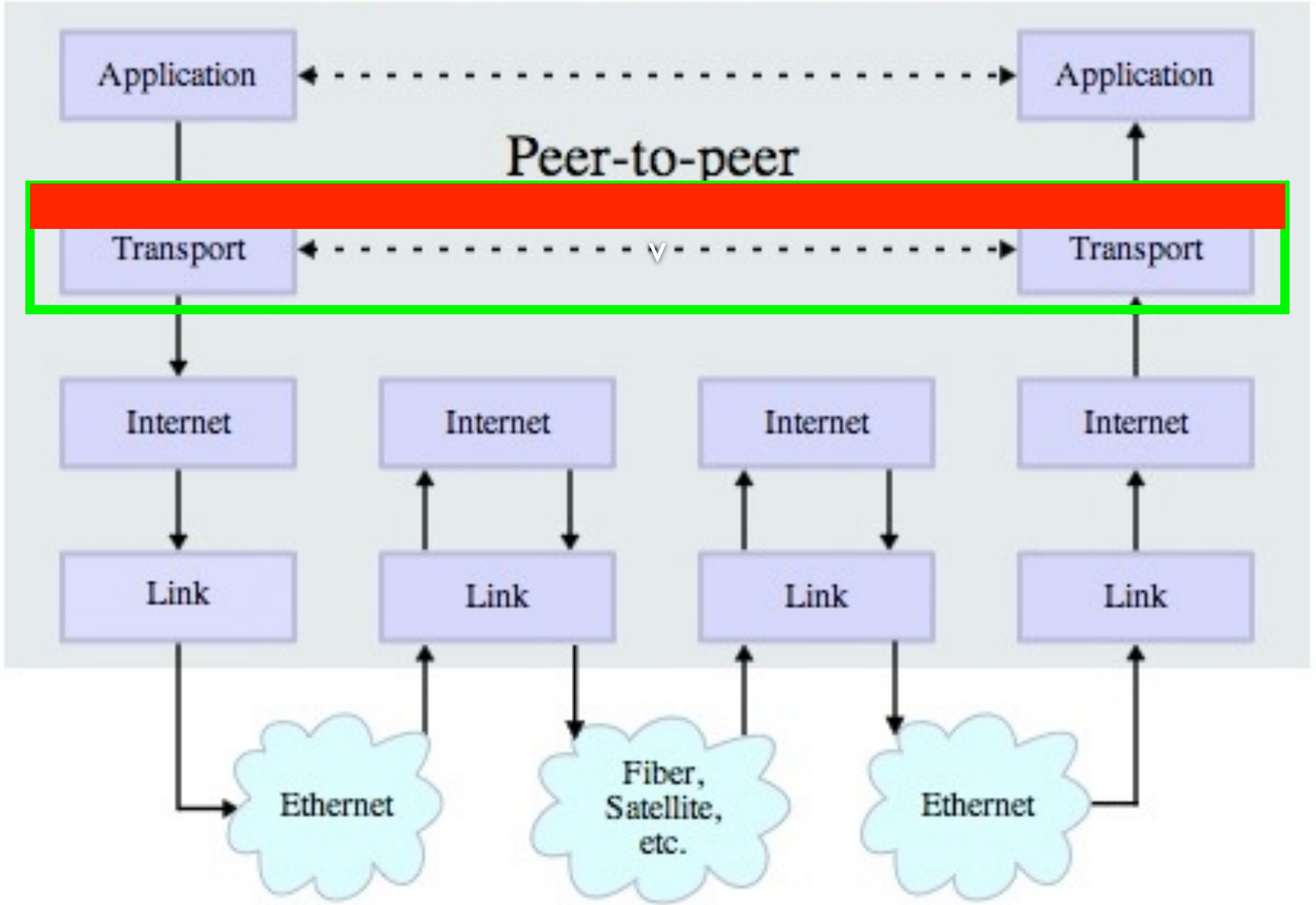
One second ago

Certificate Authority (CA)

A certificate authority is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. A CA is a trusted third party that is trusted by both the owner of the certificate and the party relying upon the certificate.

http://en.wikipedia.org/wiki/Certificate_authority

Stack Connections



Summary

- Message Confidentiality / Message Integrity
- Encrypting / Decrypting
- Message digests and message signing
- Shared Secret Key / Public Private Key

Gambling with Secrets: http://www.youtube.com/playlist?list=PLB4D701646DAF0817