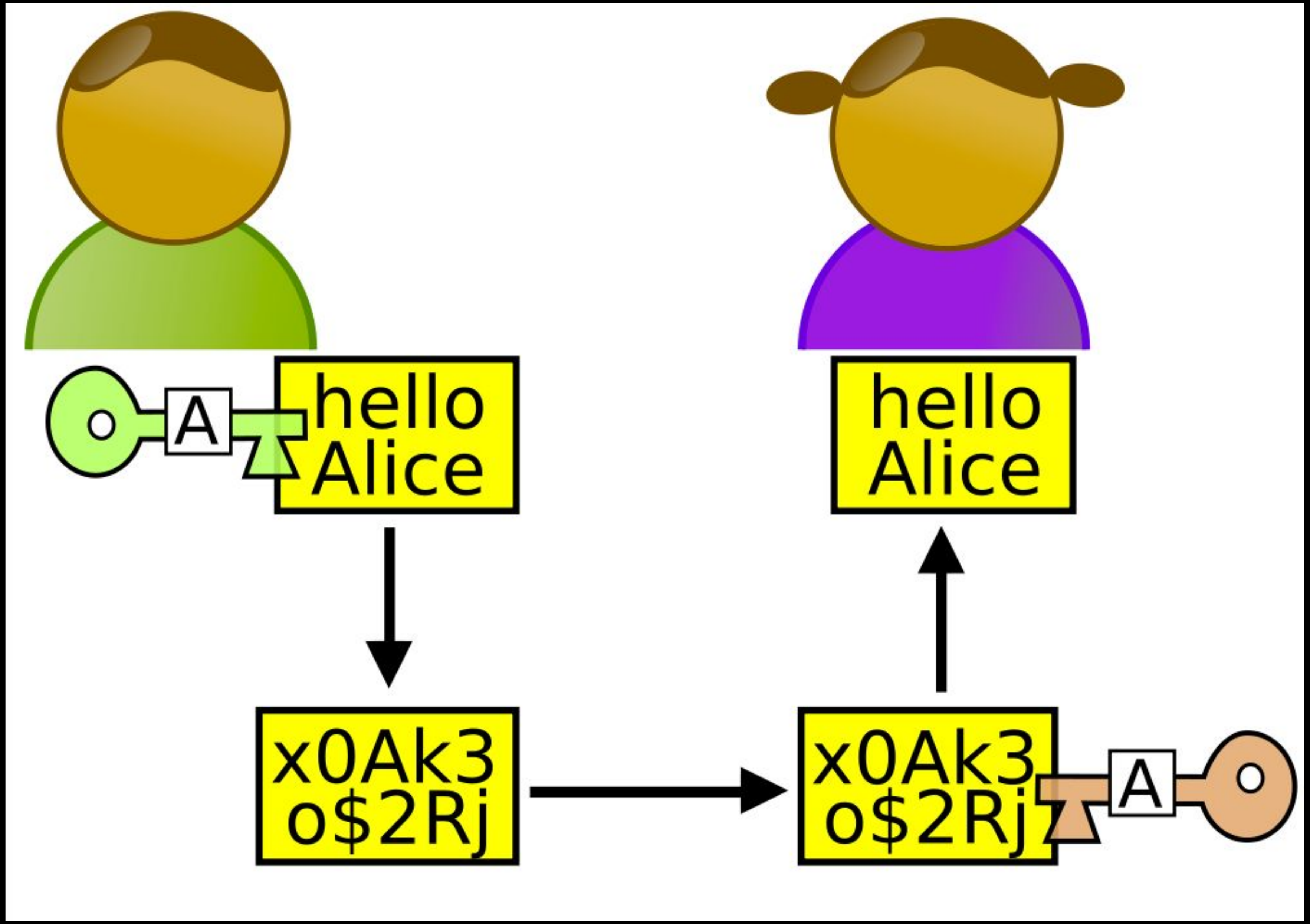
Security

Charles Severance

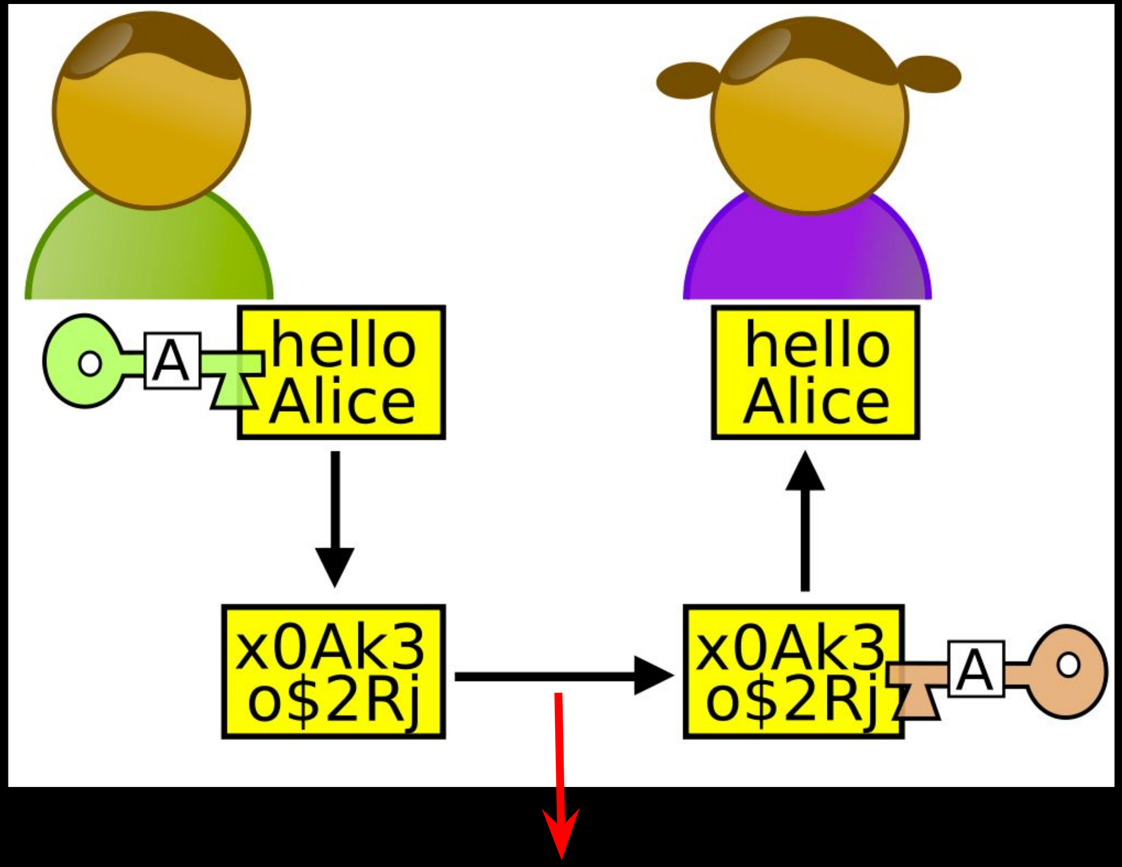
Lets Meet some Nice People



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.*



```
80/tcp     open        http
# 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="Z10N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z10N0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password:
```

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

Paranoia

- Who is out to get you?

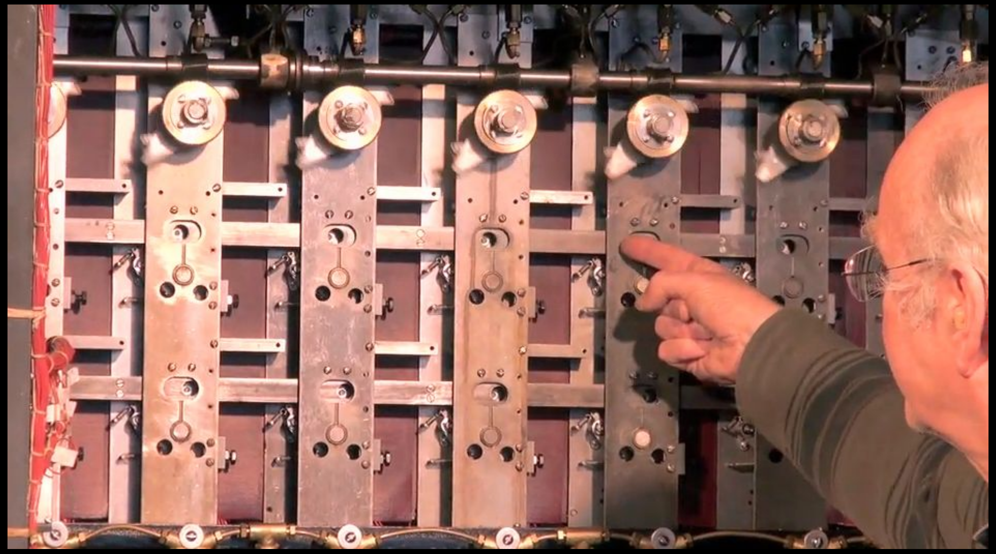
- If you are interesting or influential people want to get into your personal info.

- If you are normal, folks want to use your resources or take your information to make money…

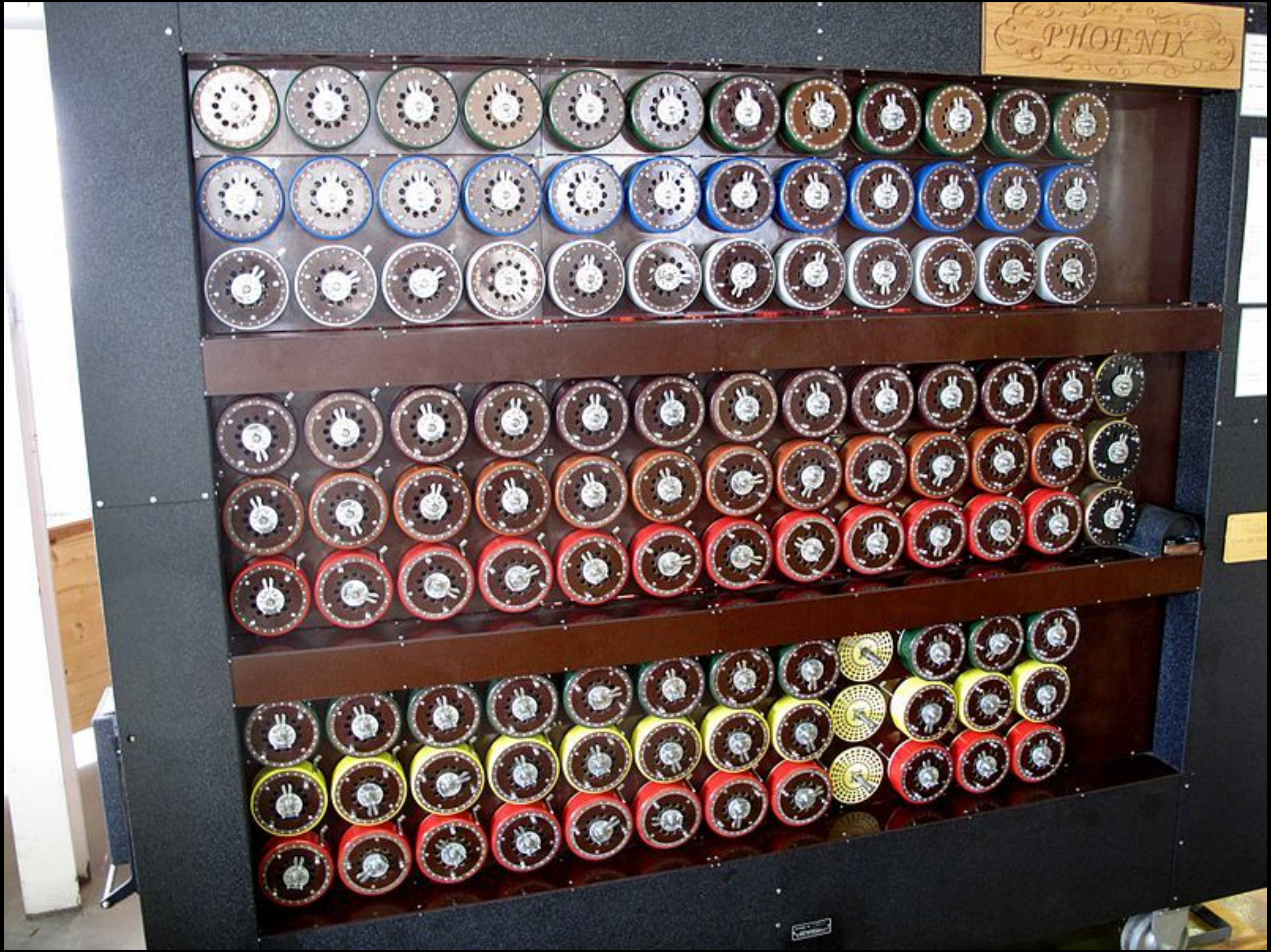
- Usually no one cares… But it is safest to assume some is always trying…

Alan Turing and Bletchley Park

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

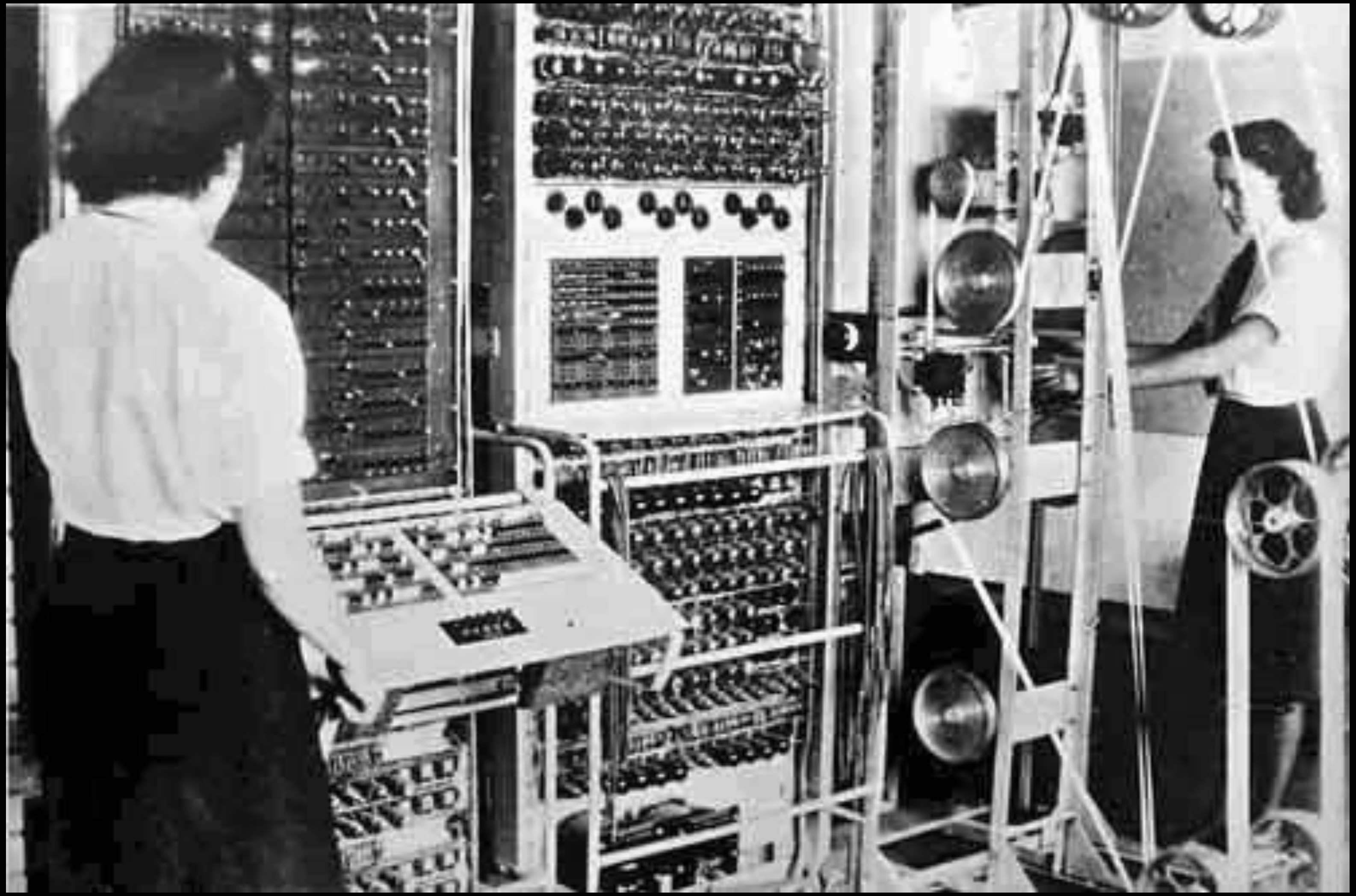


http://www.youtube.com/watch?v=5nK_ft0Lf1s



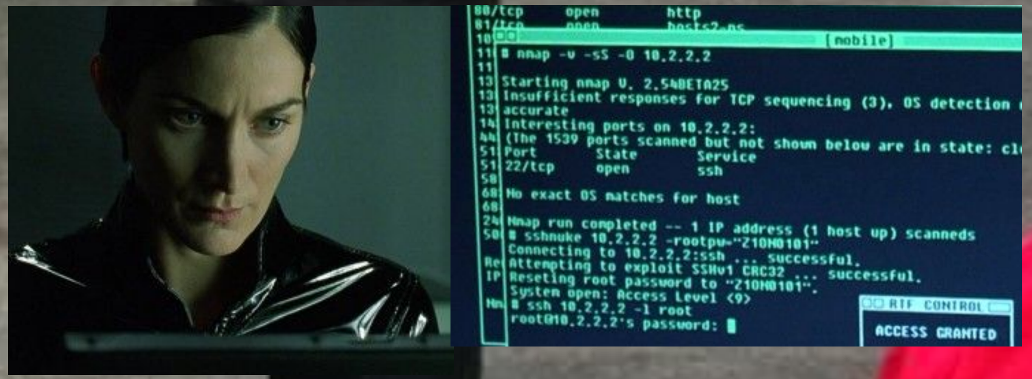
http://en.wikipedia.org/wiki/Bombe

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



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

http://nmap.org/movies.html



```
80/tcp      open        http
81/tcp      open        hosts2-ns
                                        [mobile]
# 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.
Reseting root password to "Z1ON0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password: █
```

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

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

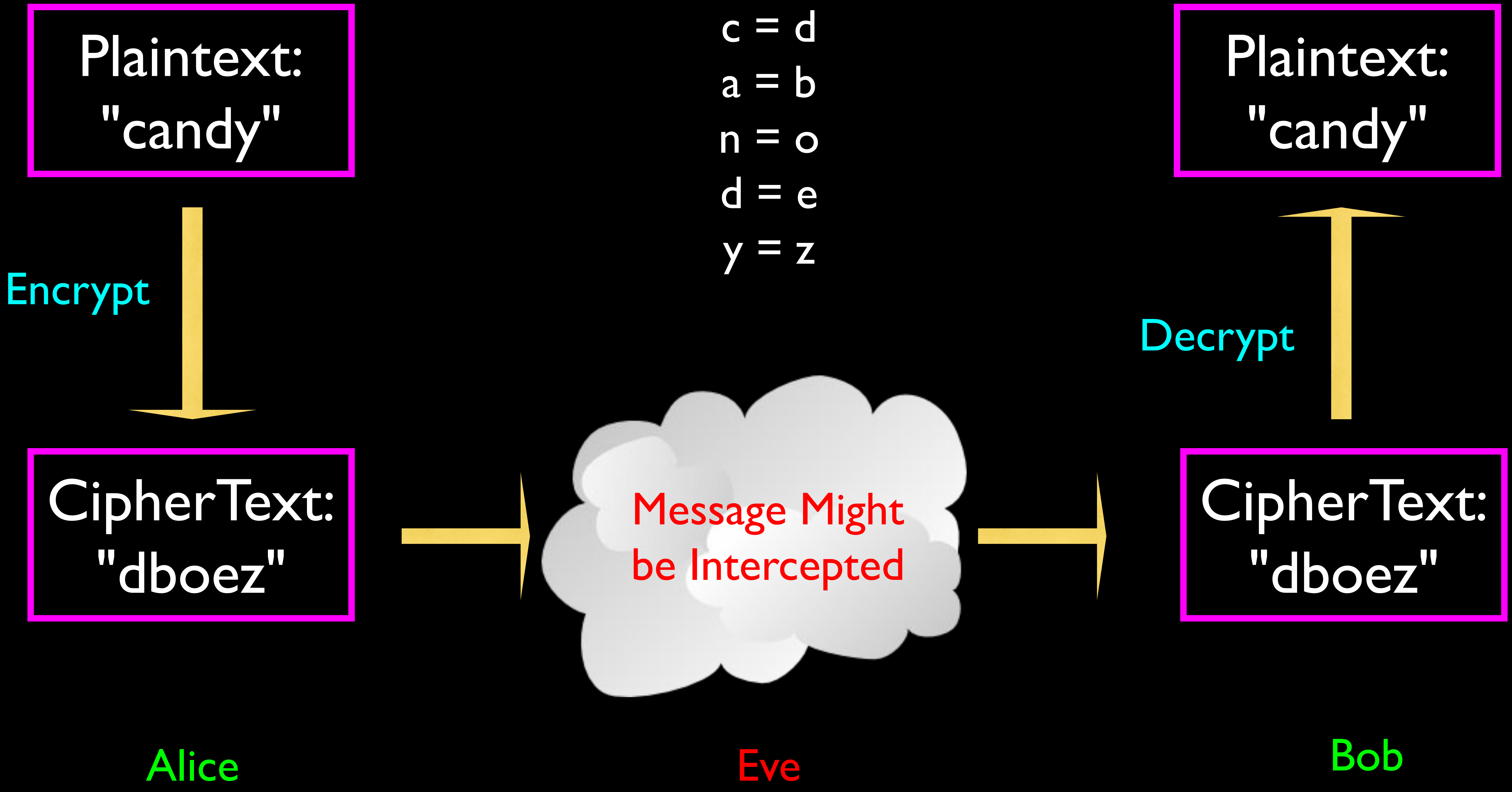
- The transformation of plaintext to ciphertext is referred to as encryption.

- 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"

Encrypt

CipherText:
"dboez"

c = d
a = b
n = o
d = e
y = z

Message Might
be Intercepted

CipherText:
"dboez"

Decrypt

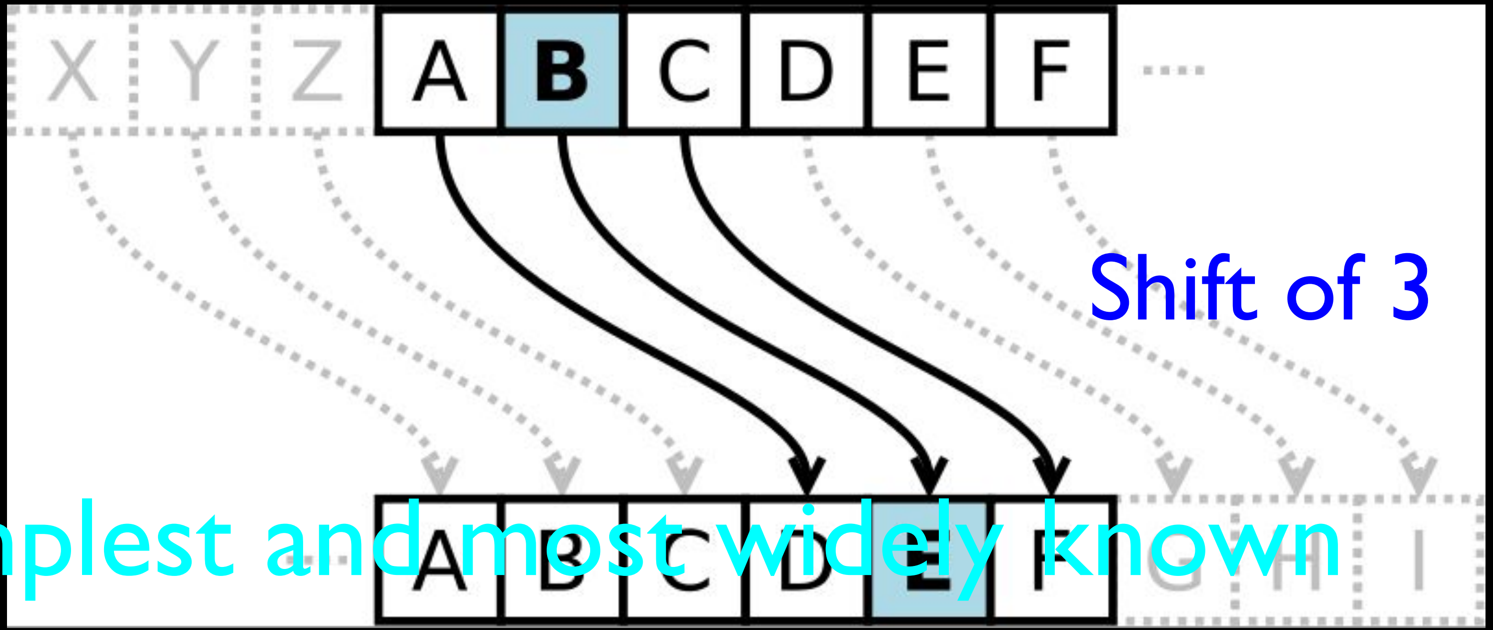
Plaintext:
"candy"

Alice

Eve

Bob

Caeser Cipher



Shift of 3

Caesar cipher is one of the simplest and most widely known encryptionCaesar cipher is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which 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 II

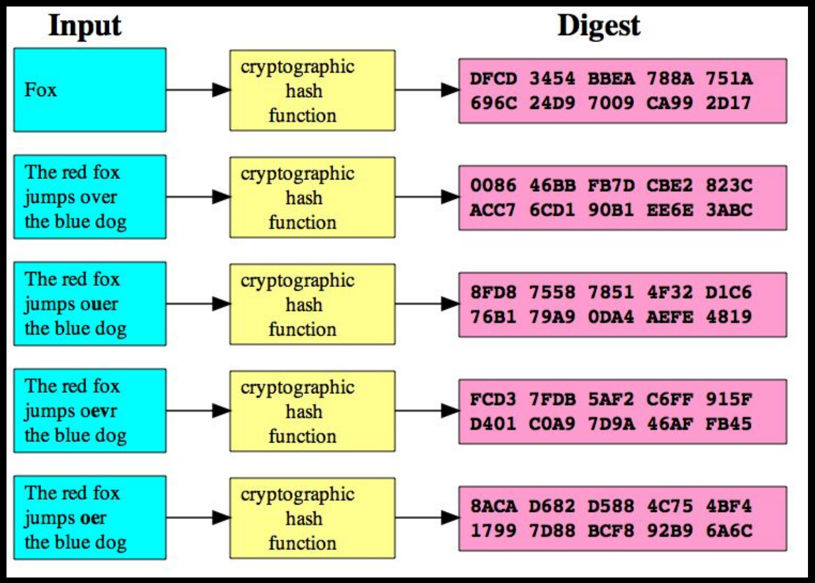
Uryyb, zl anzr vf Puhpx naq V arrq zbarl naq n wrg.

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



Input

Digest

Fox → cryptographic hash function → DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17

The red fox jumps over the blue dog → cryptographic hash function → 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC

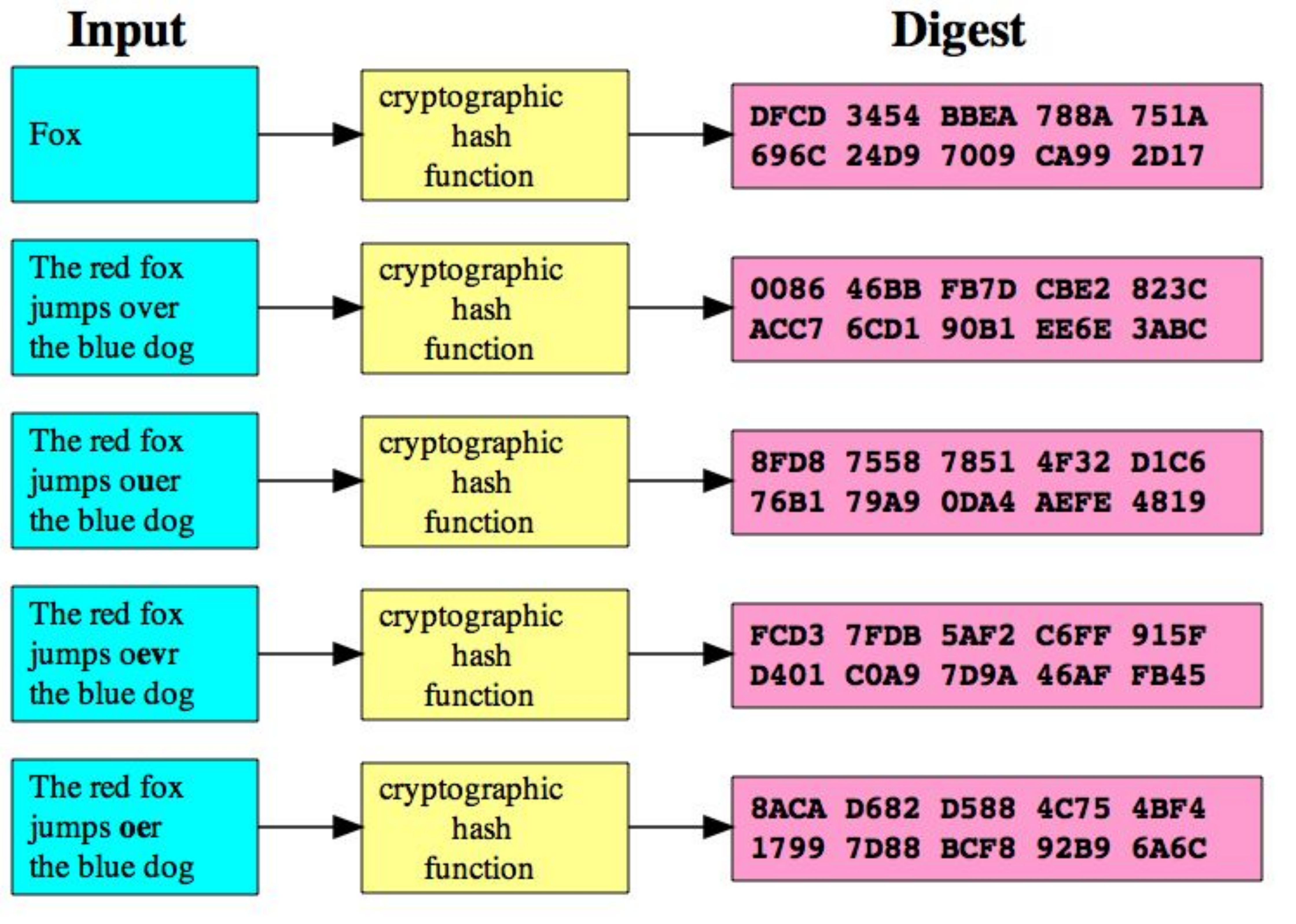
The red fox jumps ouer the blue dog → cryptographic hash function → 8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819

The red fox jumps oevr the blue dog → cryptographic hash function → FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45

The red fox jumps oer the blue dog → cryptographic hash function → 8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

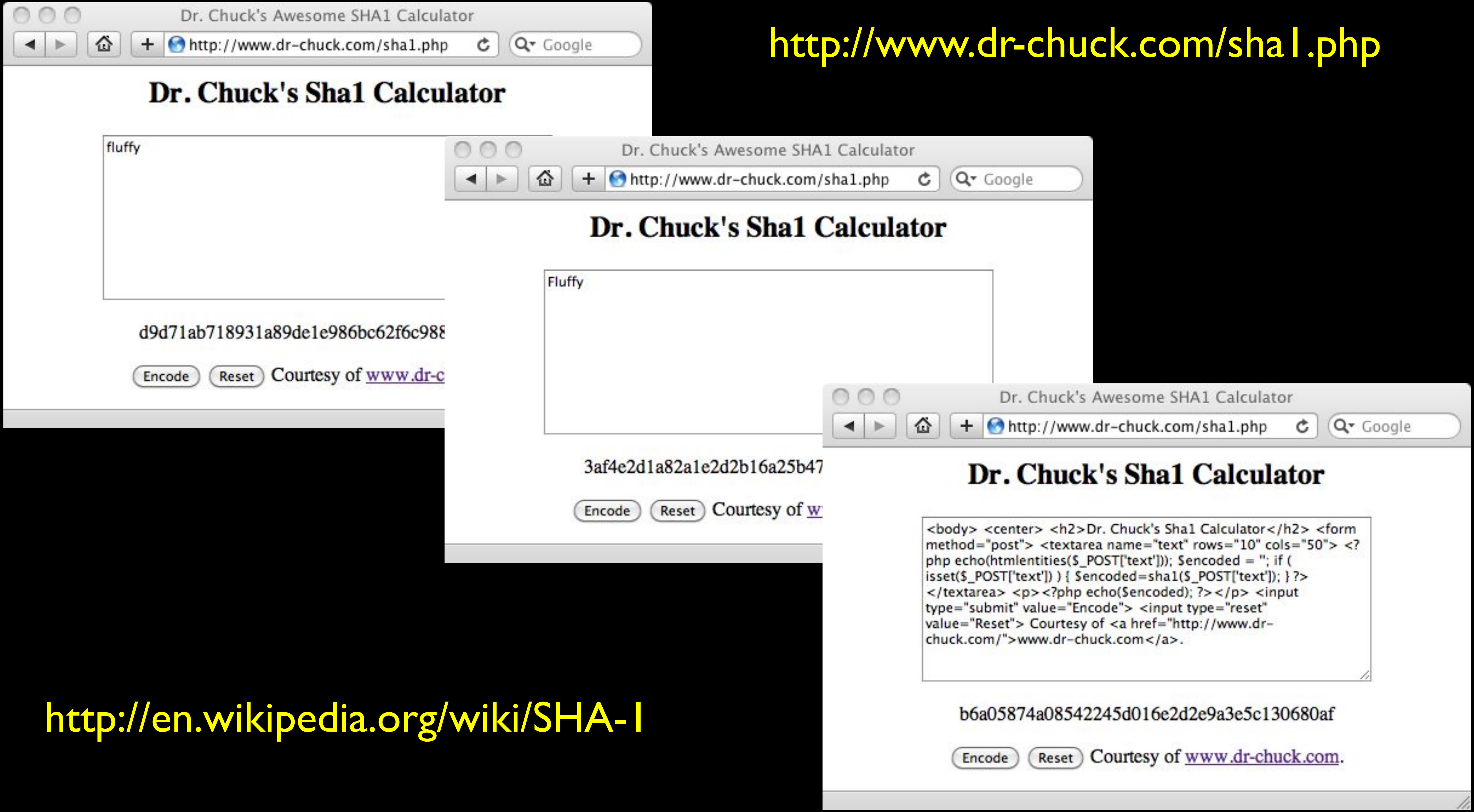
A cryptographic hash function is a function that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the " ," and the hash value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

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


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

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

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


Dr. Chuck's Awesome SHA1 Calculator
http://www.dr-chuck.com/sha1.php
Google

Dr. Chuck's Sha1 Calculator

fluffy

d9d71ab718931a89de1e986bc62f6c988

Courtesy of www.dr-c

Dr. Chuck's Awesome SHA1 Calculator
http://www.dr-chuck.com/sha1.php
Google

Dr. Chuck's Sha1 Calculator

Fluffy

3af4e2d1a82a1e2d2b16a25b47

Courtesy of w

Dr. Chuck's Awesome SHA1 Calculator
http://www.dr-chuck.com/sha1.php
Google

Dr. Chuck's Sha1 Calculator

```
<body> <center> <h2>Dr. Chuck's Sha1 Calculator</h2> <form
method="post"> <textarea name="text" rows="10" cols="50"> <?
php echo(htmlentities($_POST['text'])); $encoded = ''; if (
isset($_POST['text']) ) { $encoded=sha1($_POST['text']); } ?>
</textarea> <p><?php echo($encoded); ?></p> <input
type="submit" value="Encode"> <input type="reset"
value="Reset"> Courtesy of <a href="http://www.dr-
chuck.com/">www.dr-chuck.com</a>.
```

b6a05874a08542245d016e2d2e9a3e5c130680af

Courtesy of www.dr-chuck.com.

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

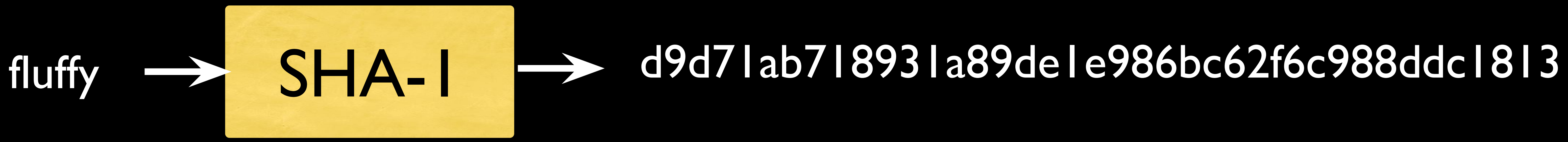
- When you set the password, they compute a hash and store the hash

- 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!

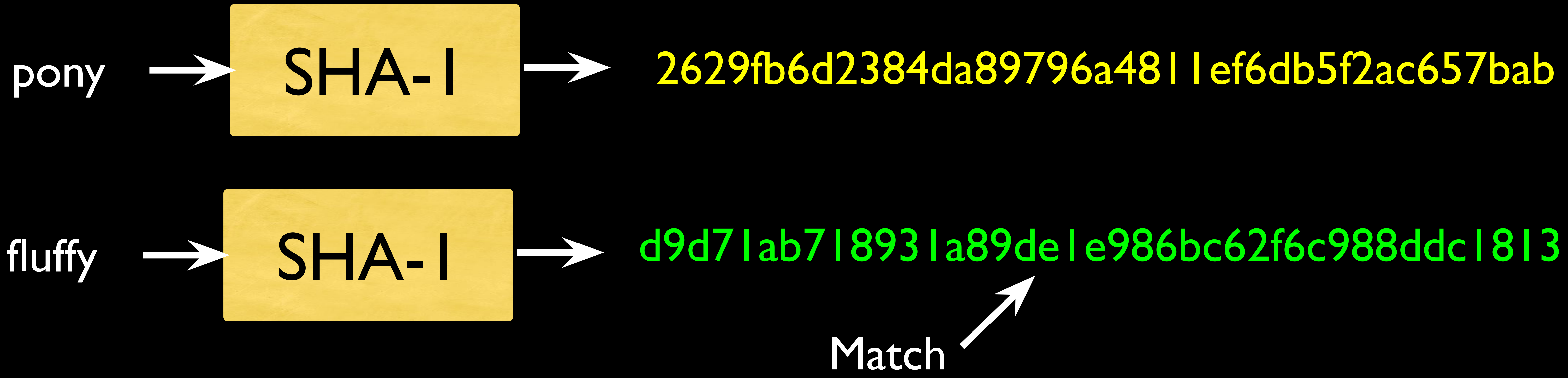
Setting a new password

Store the 'hashed password' in the database.



fluffy → SHA-1 → d9d71ab718931a89de1e986bc62f6c988ddc1813

Log in attempt



pony → SHA-1 → 2629fb6d2384da89796a4811ef6db5f2ac657bab

fluffy → SHA-1 → d9d71ab718931a89de1e986bc62f6c988ddc1813

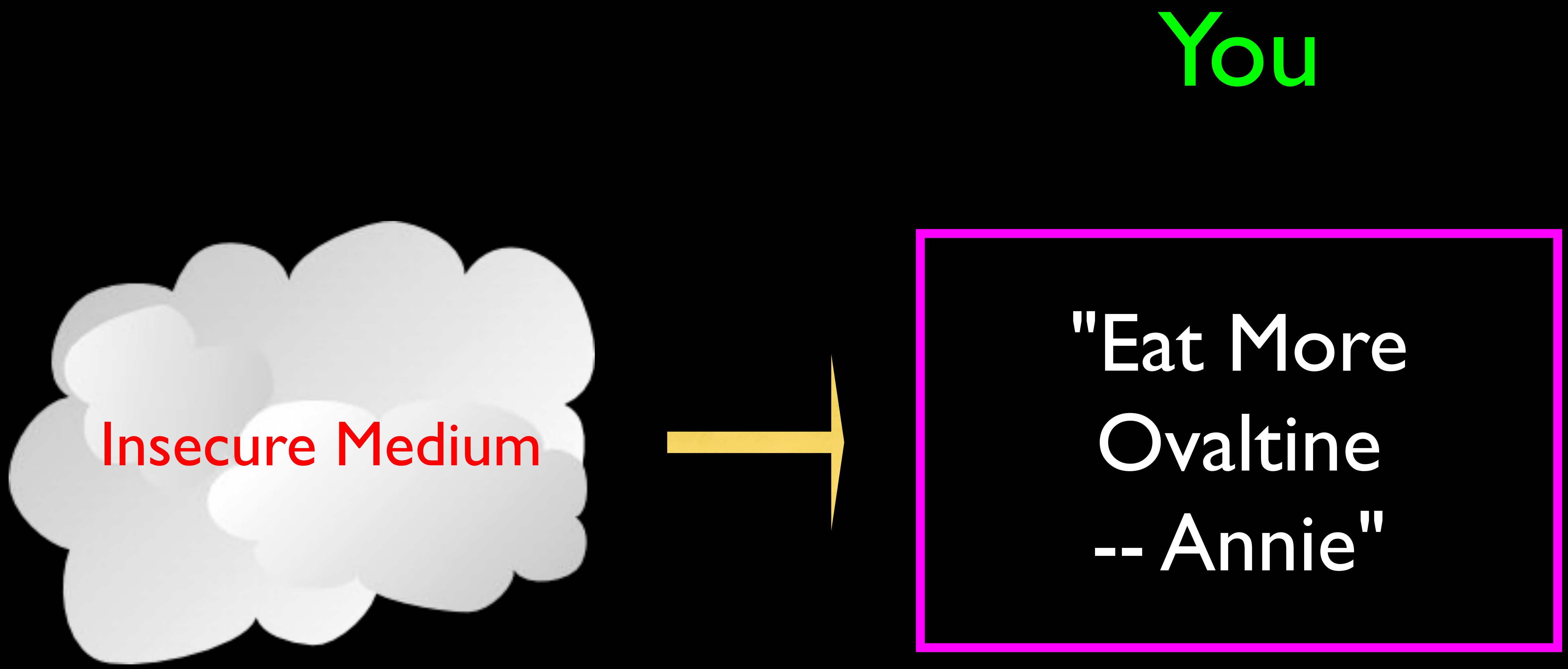
Match

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?



"Eat More
Ovaltine
-- Annie"

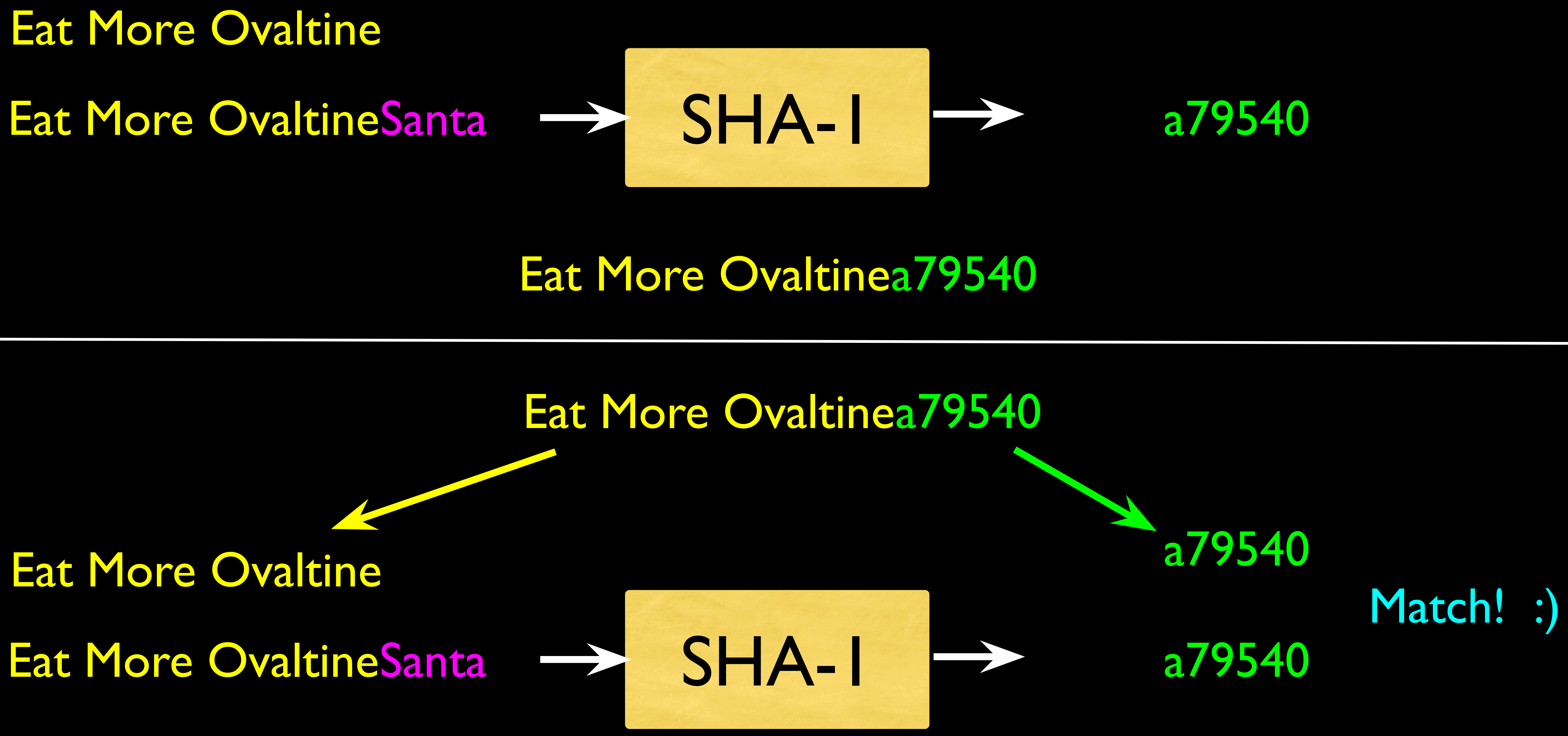
How might we be very sure this message really came from Annie and it was not altered enroute?

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



Eat More Ovaltine

Eat More OvaltineSanta

SHA-1

a79540

Eat More Ovaltinea79540

Eat More Ovaltinea79540

a79540

Eat More Ovaltine

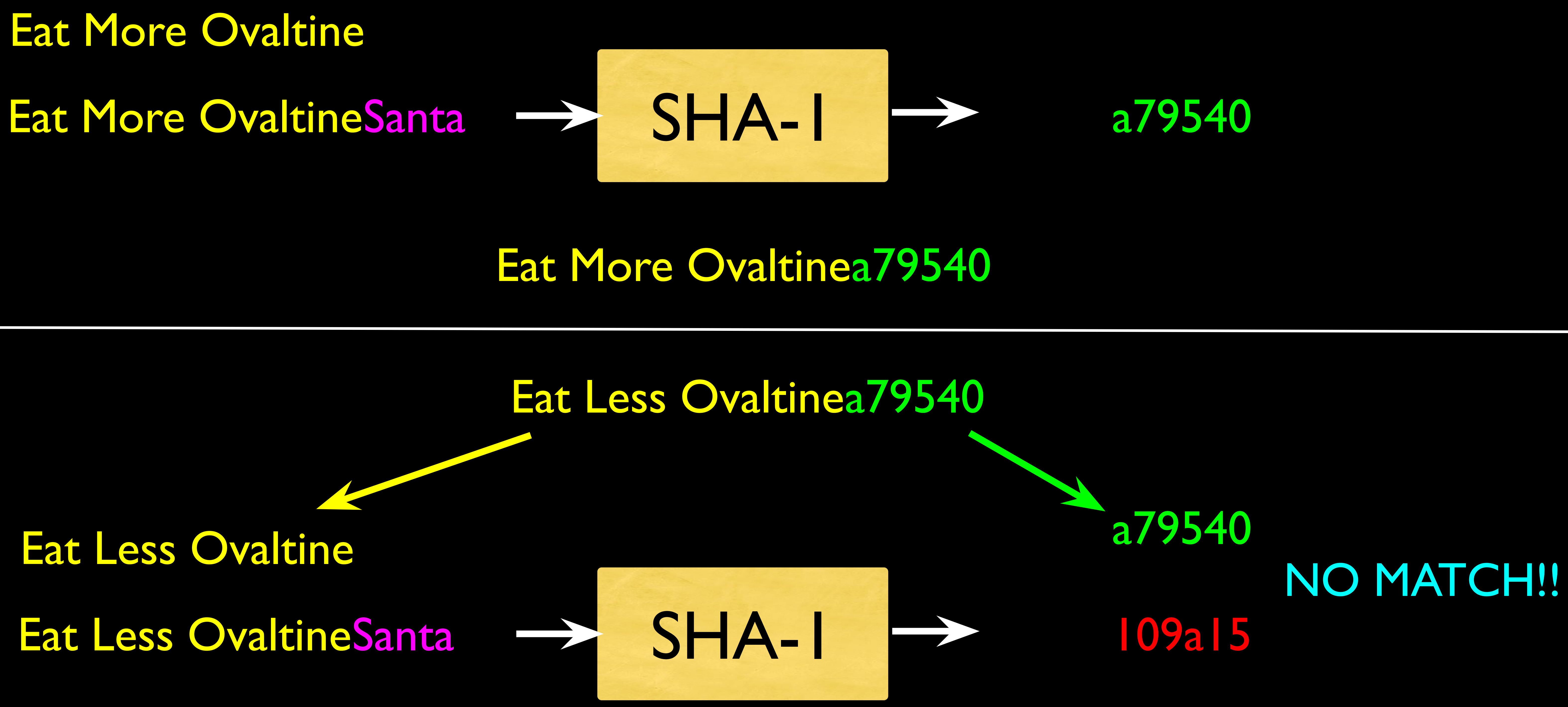
Match! :)

Eat More OvaltineSanta

SHA-1

a79540

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



Eat More Ovaltine

Eat More OvaltineSanta → SHA-1 → a79540

Eat More Ovaltinea79540

Eat Less Ovaltinea79540

Eat Less Ovaltine

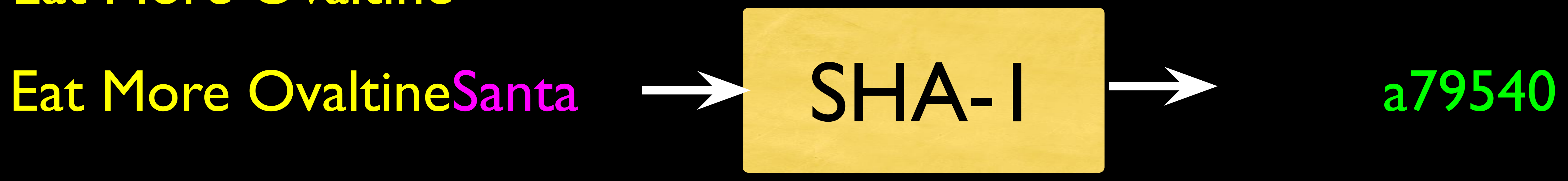
a79540

Eat Less OvaltineSanta → SHA-1 → 109a15

NO MATCH!!

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

Eat More Ovaltine



Eat More OvaltineSanta

SHA-1

a79540

Eat More Ovaltinea79540

Free Cookies84d211

Free Candy26497c

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

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

Public Key Encryption
Confidentiality

Grezvabybtl

- Pbasvqragvnyvgl
  - Cerirag hanhgubevmrq ivrjvat bs cevingr vasbezngvba
- Vagrtevgl
  - Vasbezngvba vf sebz jub lbh guvax vg vf sebz naq unf abg orra zbqvsvrq fvapr vg jnf frag

www.rot13.com

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

Public Key Encryption

- 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

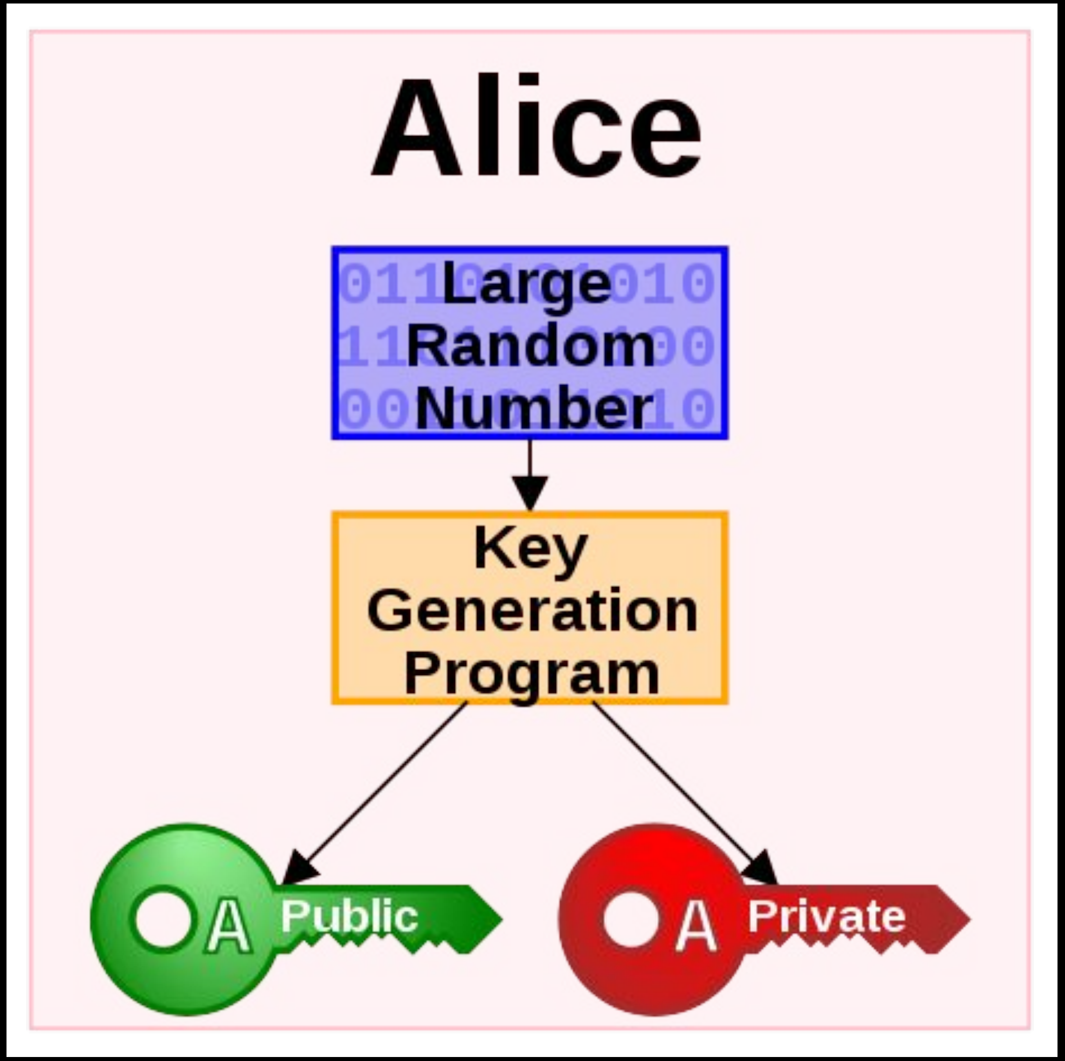
- A message encrypted with one of the keys can only be decrypted with the other key.

- 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

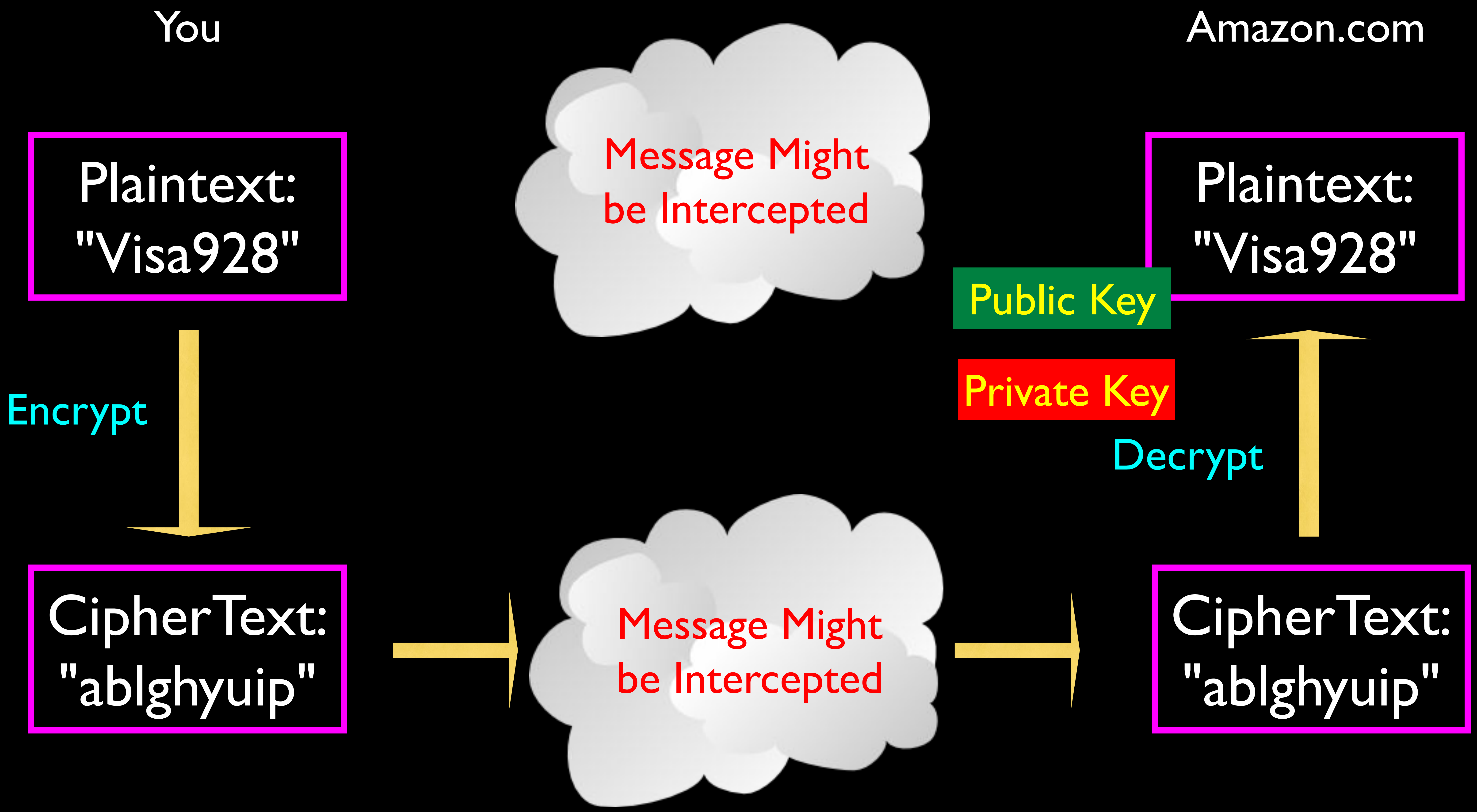
Public Key Math (light)

- 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!



You

Amazon.com

Plaintext:
"Visa928"

Encrypt

CipherText:
"ablghyuip"

Message Might
be Intercepted

Message Might
be Intercepted

Plaintext:
"Visa928"

Public Key

Private Key

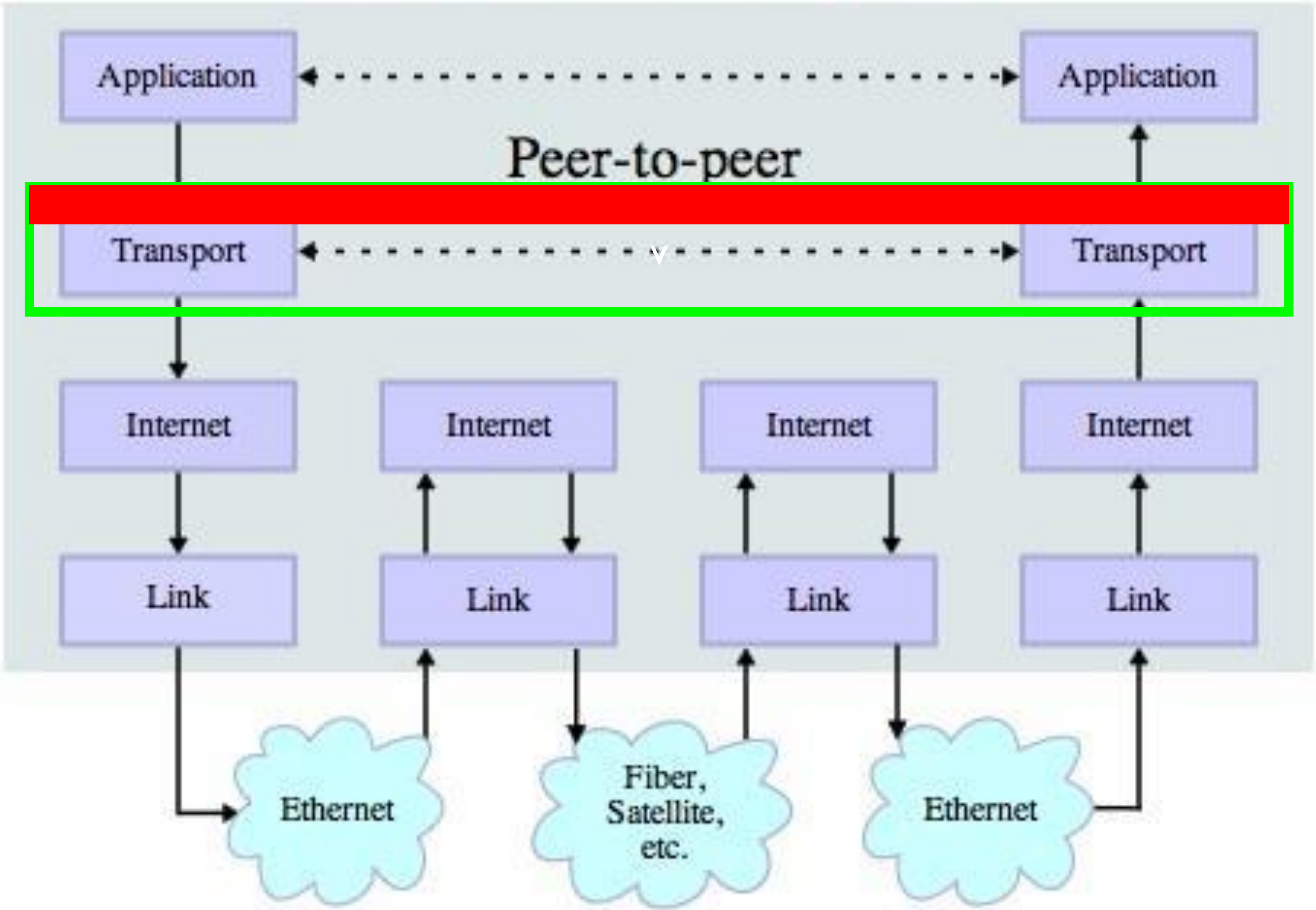
Decrypt

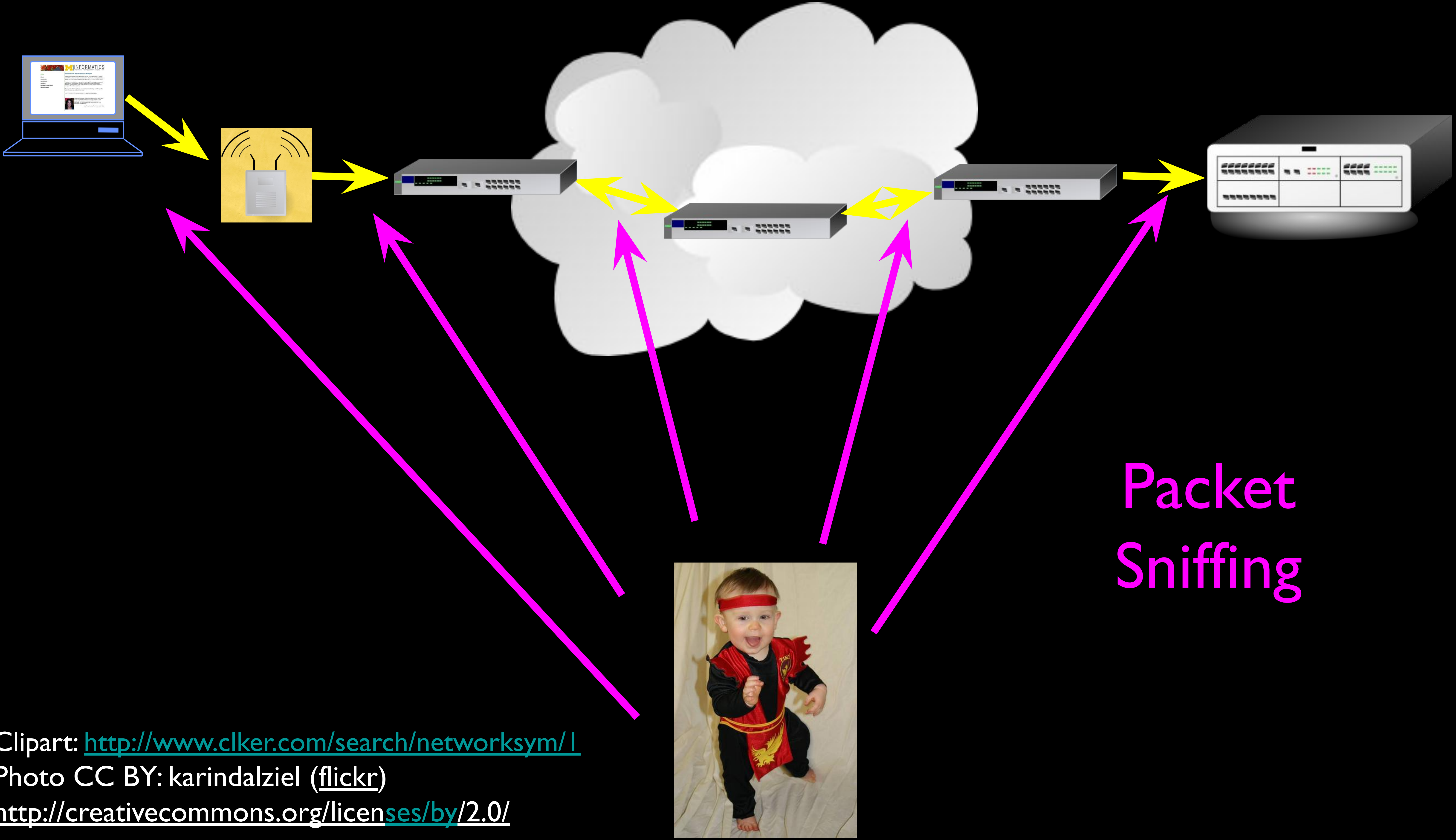
CipherText:
"ablghyuip"

Secure Sockets Layer (SSL)
Security for TCP

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

Stack Connections





Packet Sniffing

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

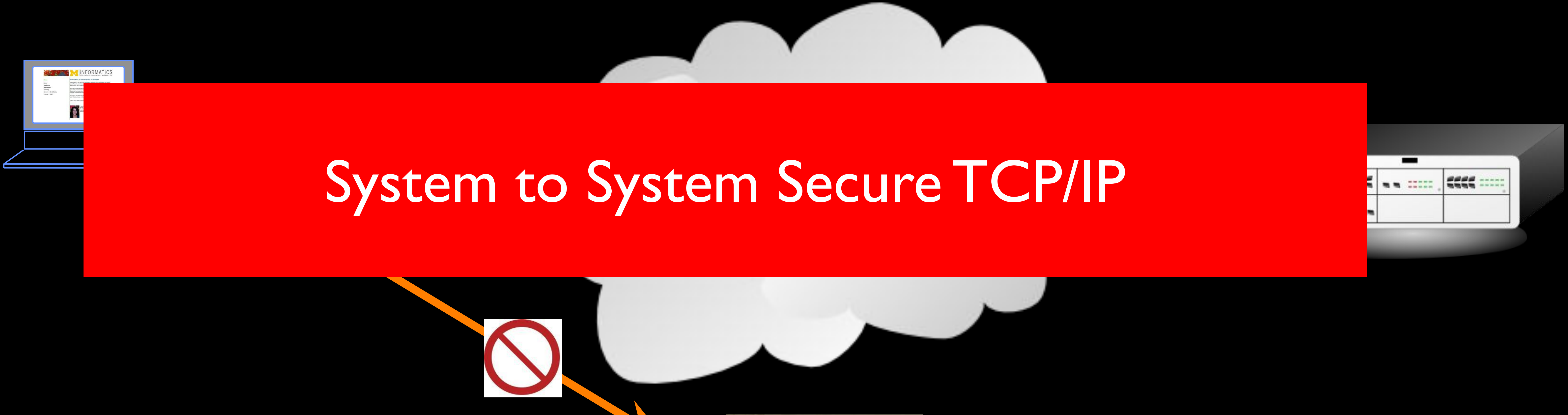
Transport Layer Security (TLS)

- 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
- Encrypting and decryption takes resources - so we use it for things when it is needed

Secure Application Protocols

- There are often secure and unencrypted application protocols
  - http://www.facebook.com
  - https://www.facebook.com
- Your browser tells you when using a secure connection - you should never type passwords into a non-secure connection
- Especially over wireless - especially at a security conference...

System to System Secure TCP/IP



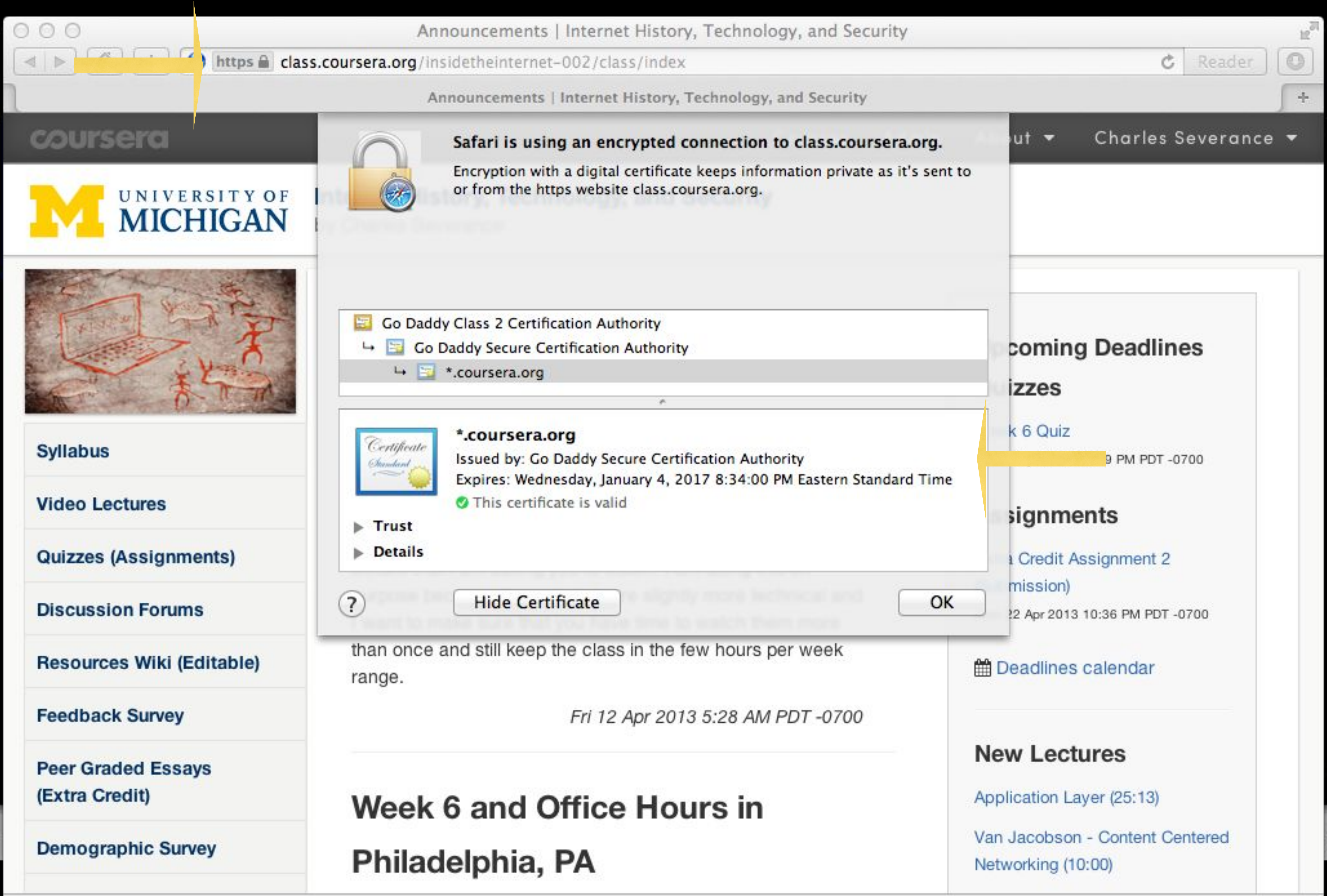
Your local connection (particularly when wireless) is your greatest exposure.

Generally, the backbone of the Internet is pretty secure to prying eyes from generic baddies...

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

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

Certificate Authorities
Integrity



Announcements | Internet History, Technology, and Security

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

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

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

Digital Certificates

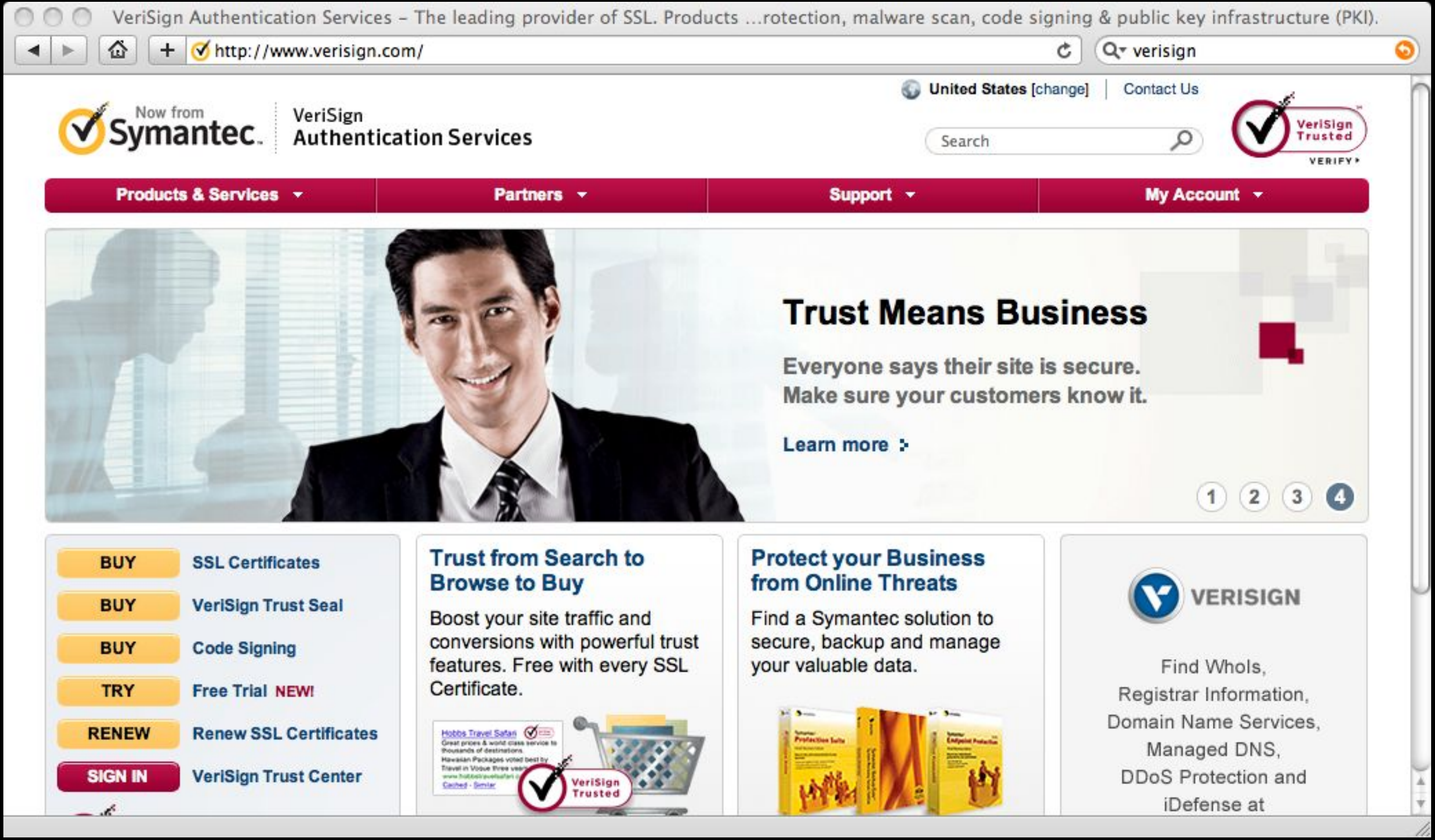
In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind a p which uses a digital signature to bind a public key with an identity — information such as the name of a person or an organization, 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

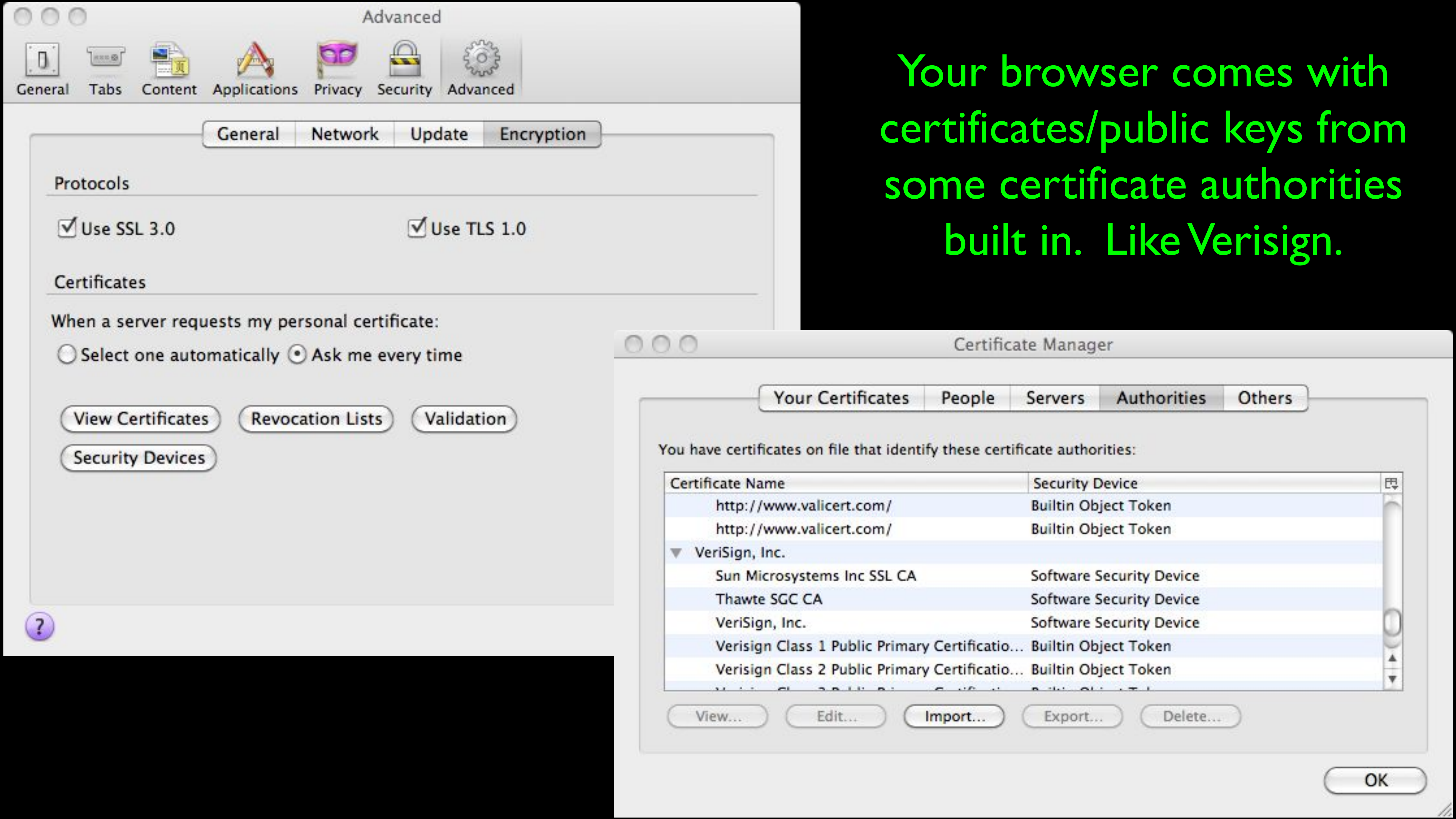
Certificate Authority (CA)

A certificate authority is an entity that issues digital certificatesA 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



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



Protocols

☑ Use SSL 3.0   ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

You have certificates on file that identify these certificate authorities:

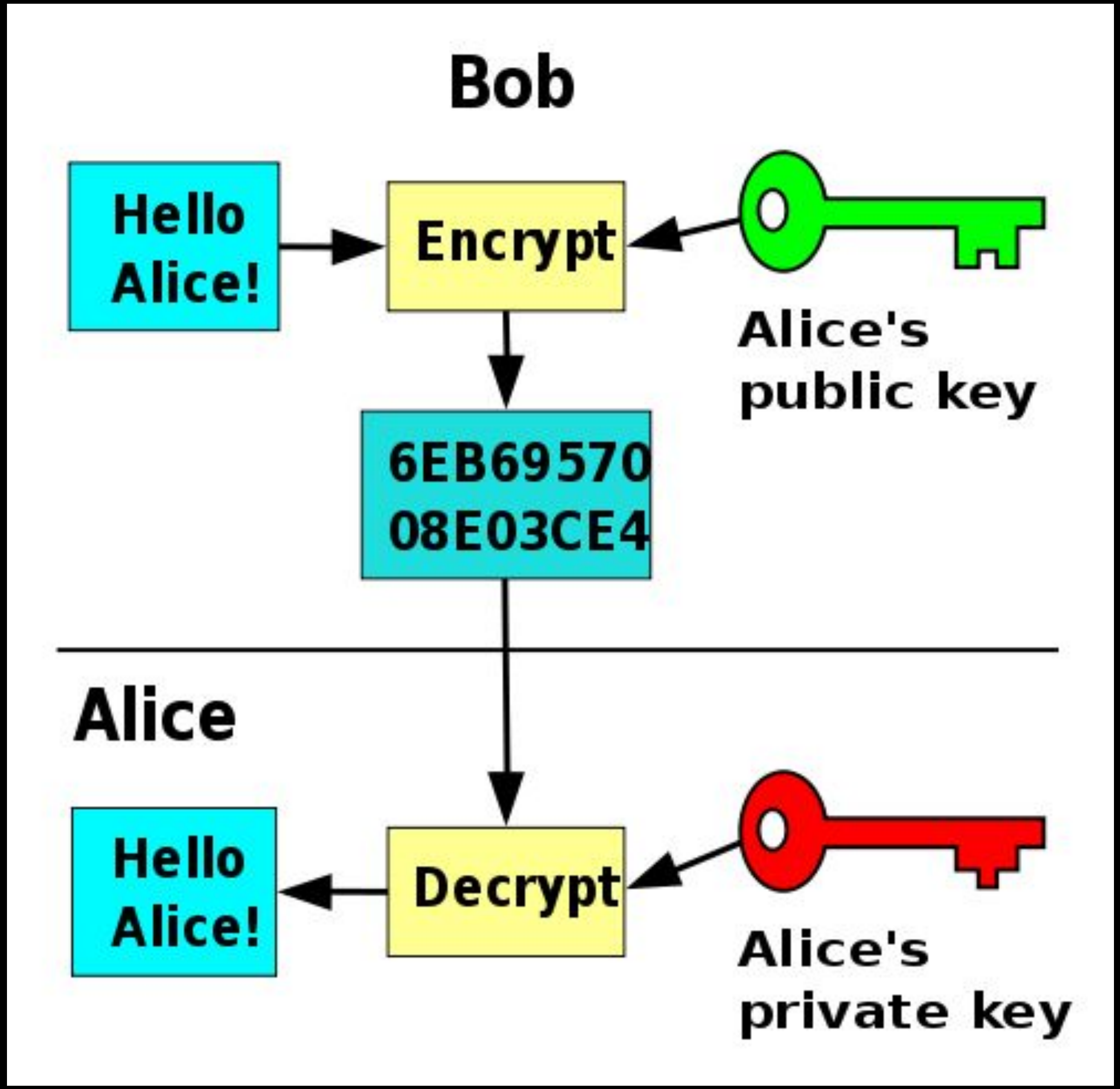
Certificate Name	Security Device
http://www.valicert.com/	Builtin Object Token
http://www.valicert.com/	Builtin Object Token
▼ VeriSign, Inc.	
Sun Microsystems Inc SSL CA	Software Security Device
Thawte SGC CA	Software Security Device
VeriSign, Inc.	Software Security Device
Verisign Class 1 Public Primary Certificatio...	Builtin Object Token
Verisign Class 2 Public Primary Certificatio...	Builtin Object Token

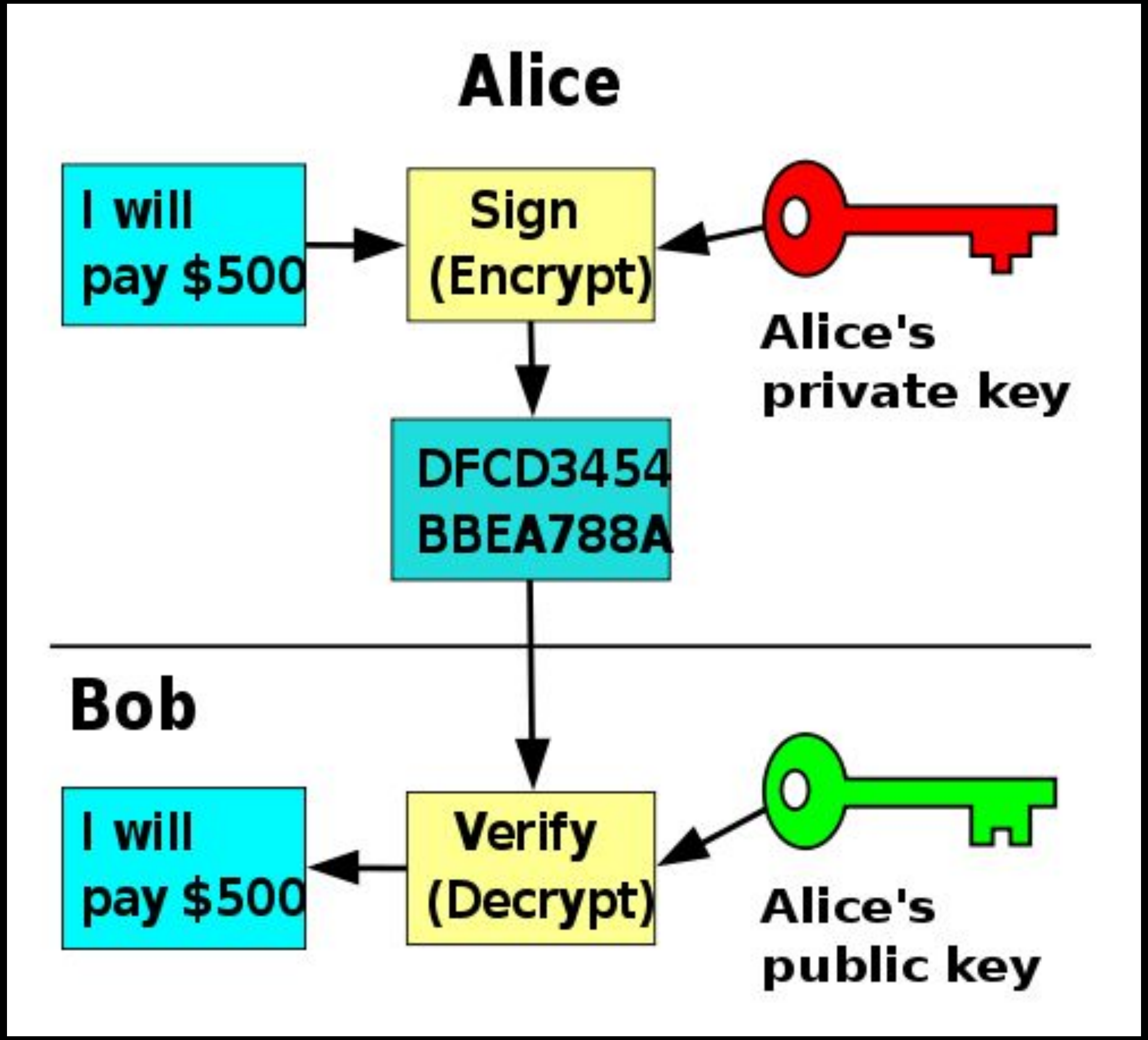
Public-Key Issues

- 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

Public/Private Keys for Signing





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

Digital Certificates

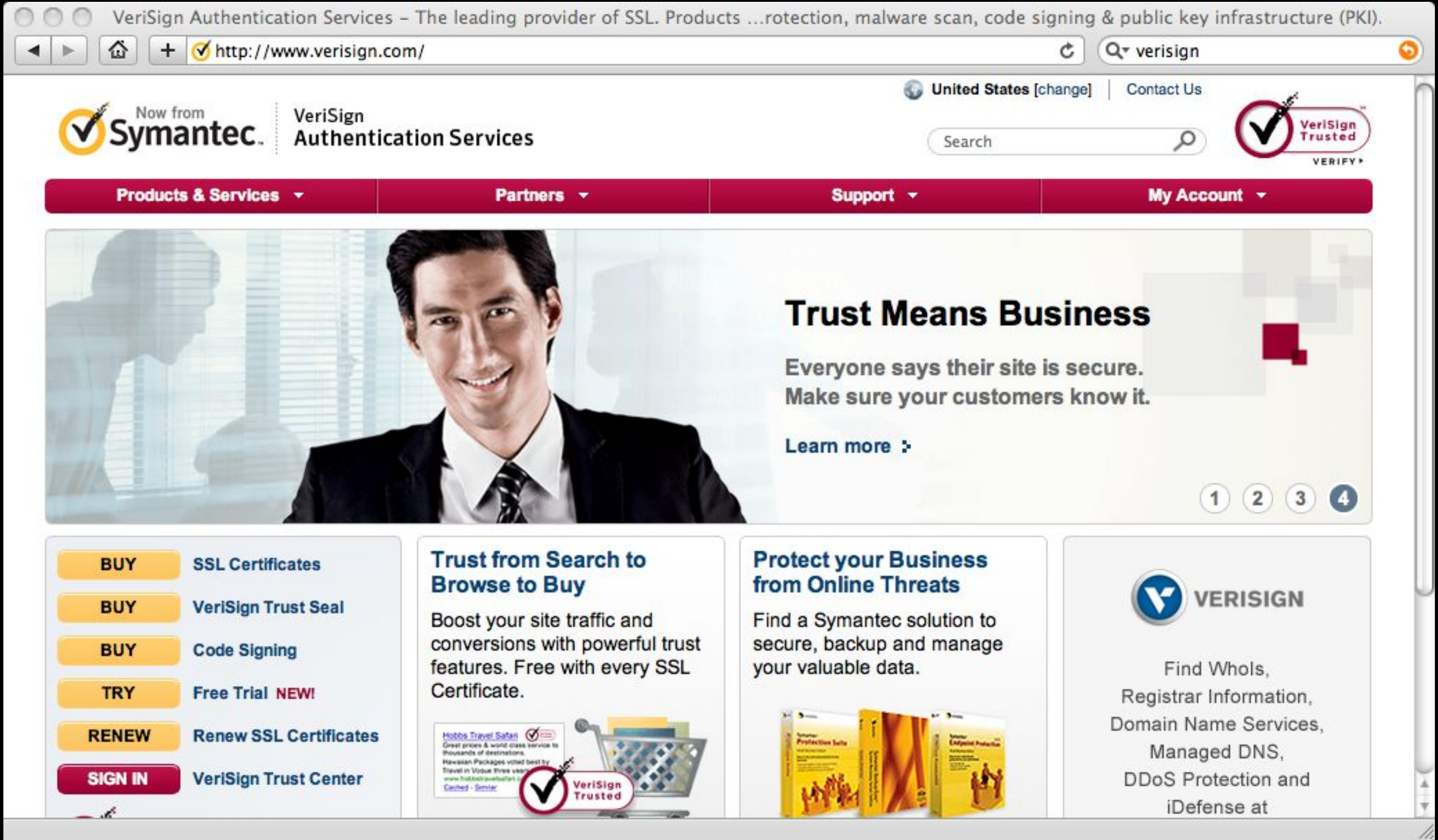
In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind a p which uses a digital signature to bind a public key with an identity — information such as the name of a person or an organization, 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 certificatesA 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



Trust Means Business

Everyone says their site is secure.
Make sure your customers know it.

Learn more

SSL Certificates

VeriSign Trust Seal

Code Signing

Free Trial NEW!

Renew SSL Certificates

VeriSign Trust Center

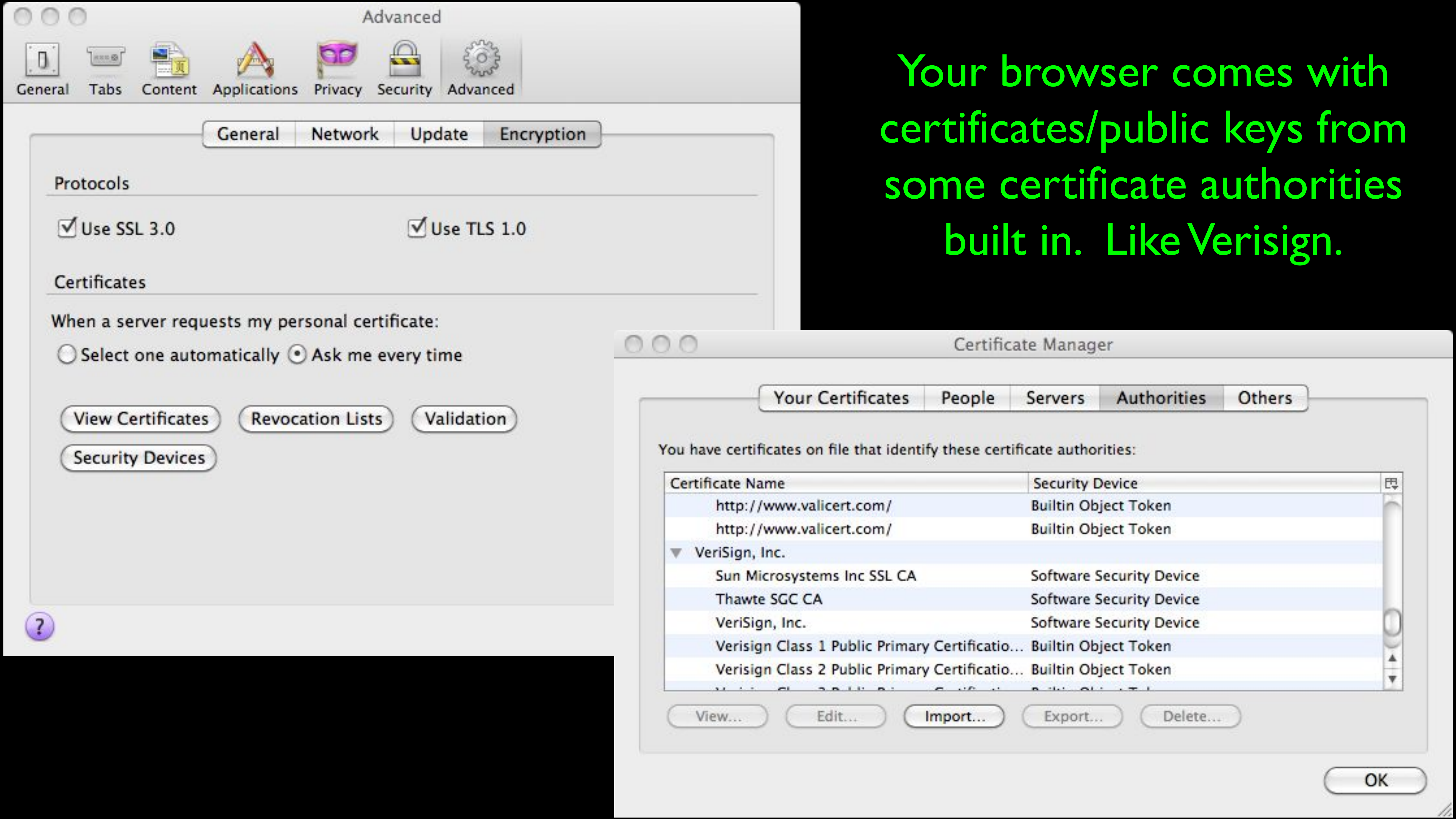
Trust from Search to Browse to Buy

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.

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



Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
http://www.valicert.com/	Builtin Object Token
http://www.valicert.com/	Builtin Object Token
▼ VeriSign, Inc.	
Sun Microsystems Inc SSL CA	Software Security Device
Thawte SGC CA	Software Security Device
VeriSign, Inc.	Software Security Device
Verisign Class 1 Public Primary Certificatio...	Builtin Object Token
Verisign Class 2 Public Primary Certificatio...	Builtin Object Token

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

How Amazon gets a public key signed by Verisign

Verisign

Verisign Private Key

Verisign Public Key

Amazon

Your Laptop

Verisign

Verisign Private Key

Cert: Amazon
-- Verisign

Amazon Public Key

Amazon Private Key

Verisign Public Key

Amazon

Your Laptop

Verisign

Verisign Private Key

Amazon Public Key

Cert: Amazon

-- Verisign

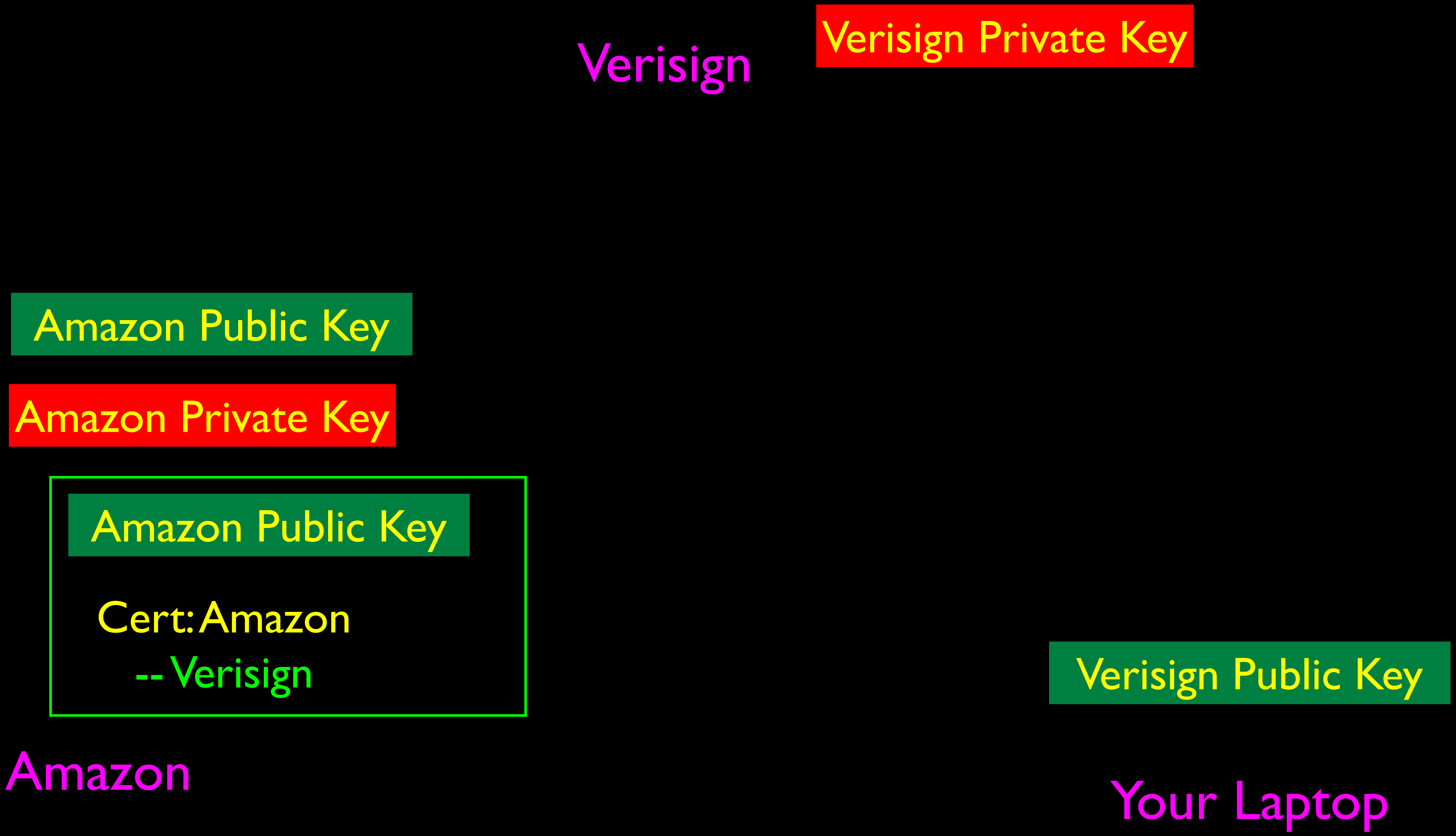
Amazon Public Key

Amazon Private Key

Verisign Public Key

Amazon

Your Laptop



Verisign

Verisign Private Key

Amazon Public Key

Amazon Private Key

Amazon Public Key

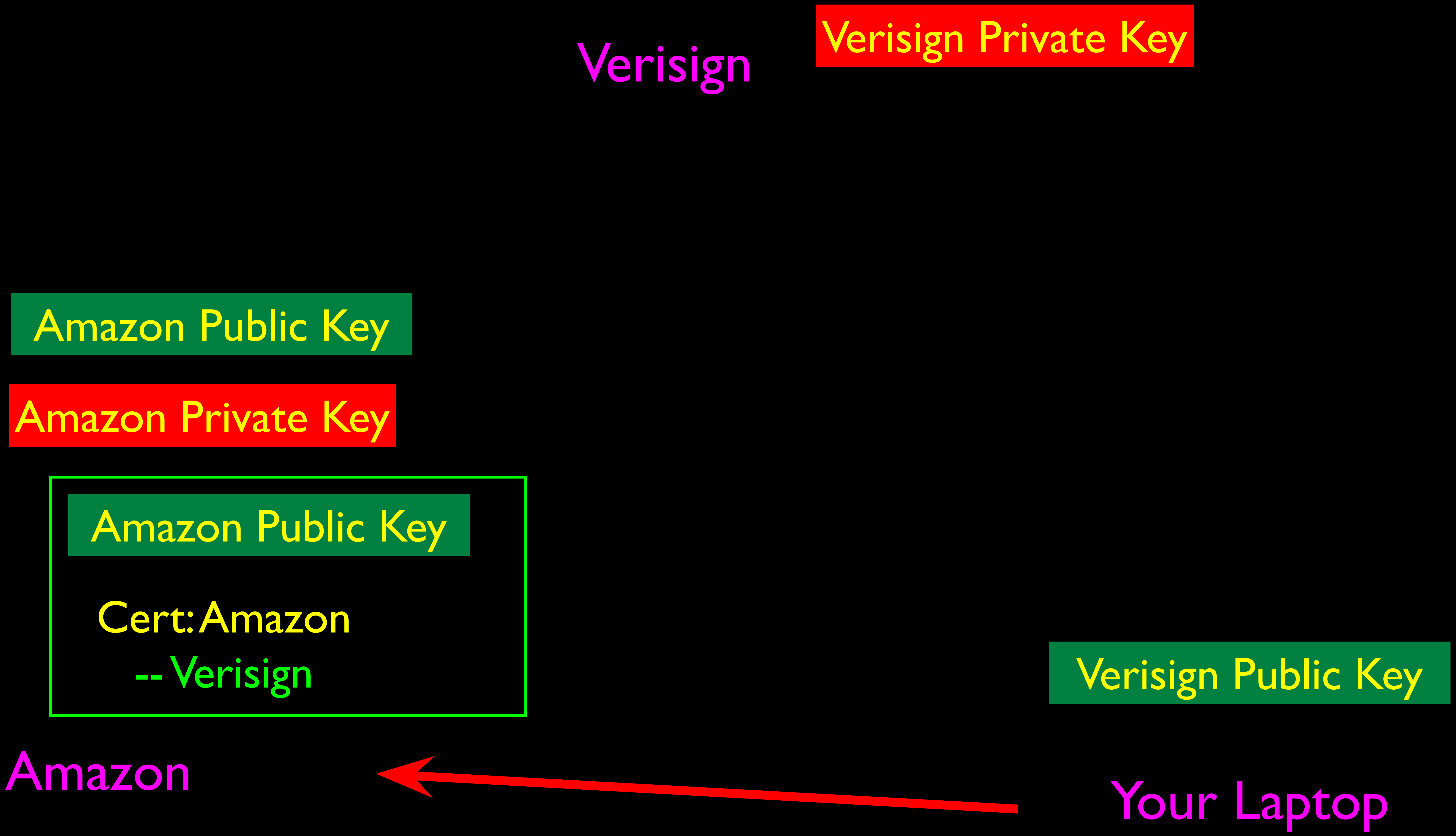
Cert: Amazon

-- Verisign

Verisign Public Key

Amazon

Your Laptop



Verisign

Verisign Private Key

Amazon Public Key

Amazon Private Key

Amazon Public Key

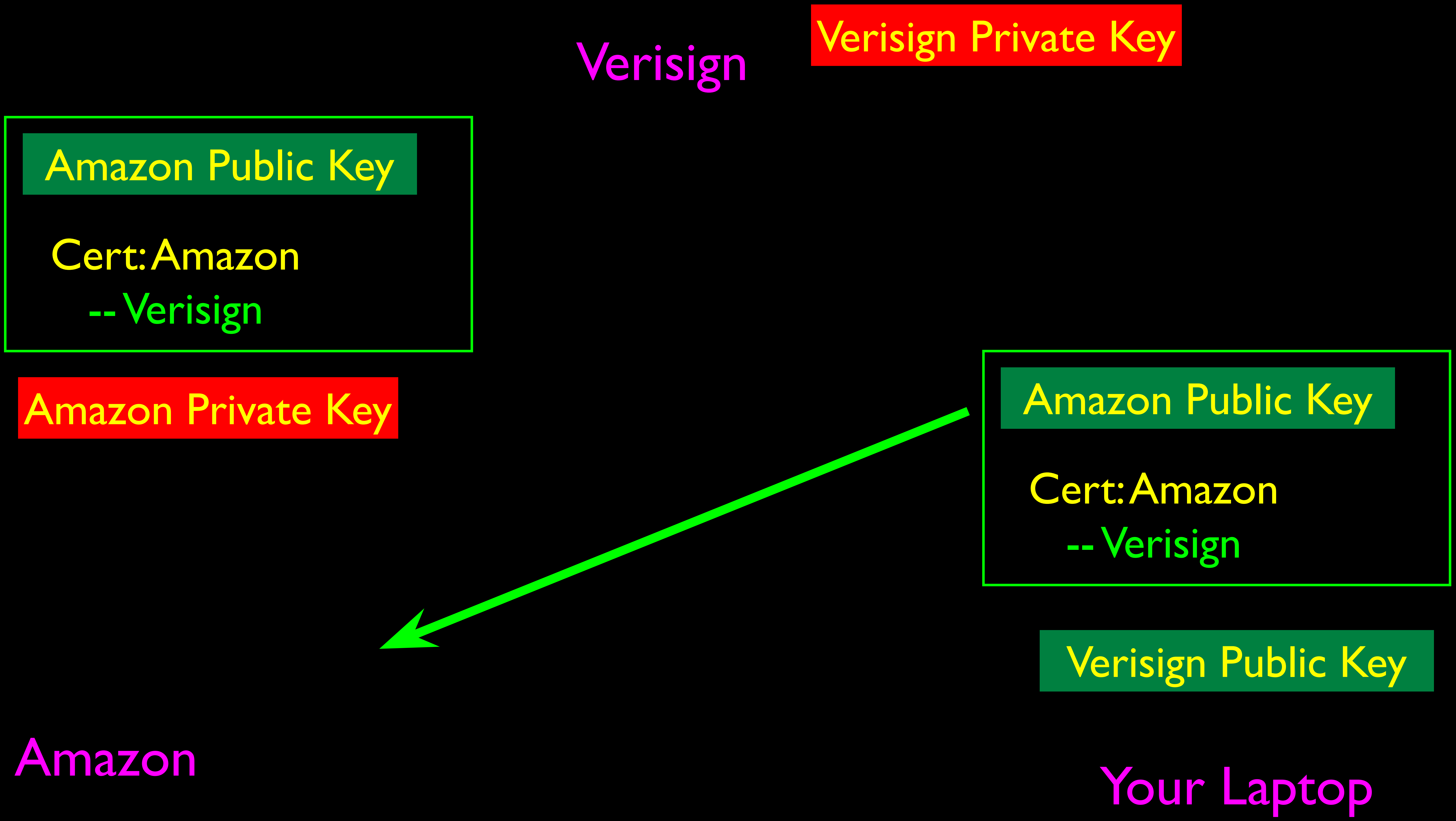
Cert: Amazon

-- Verisign

Verisign Public Key

Amazon

Your Laptop



Verisign

Verisign Private Key

Amazon Public Key

Cert: Amazon

-- Verisign

Amazon Private Key

Amazon Public Key

Cert: Amazon

-- Verisign

Verisign Public Key

Amazon

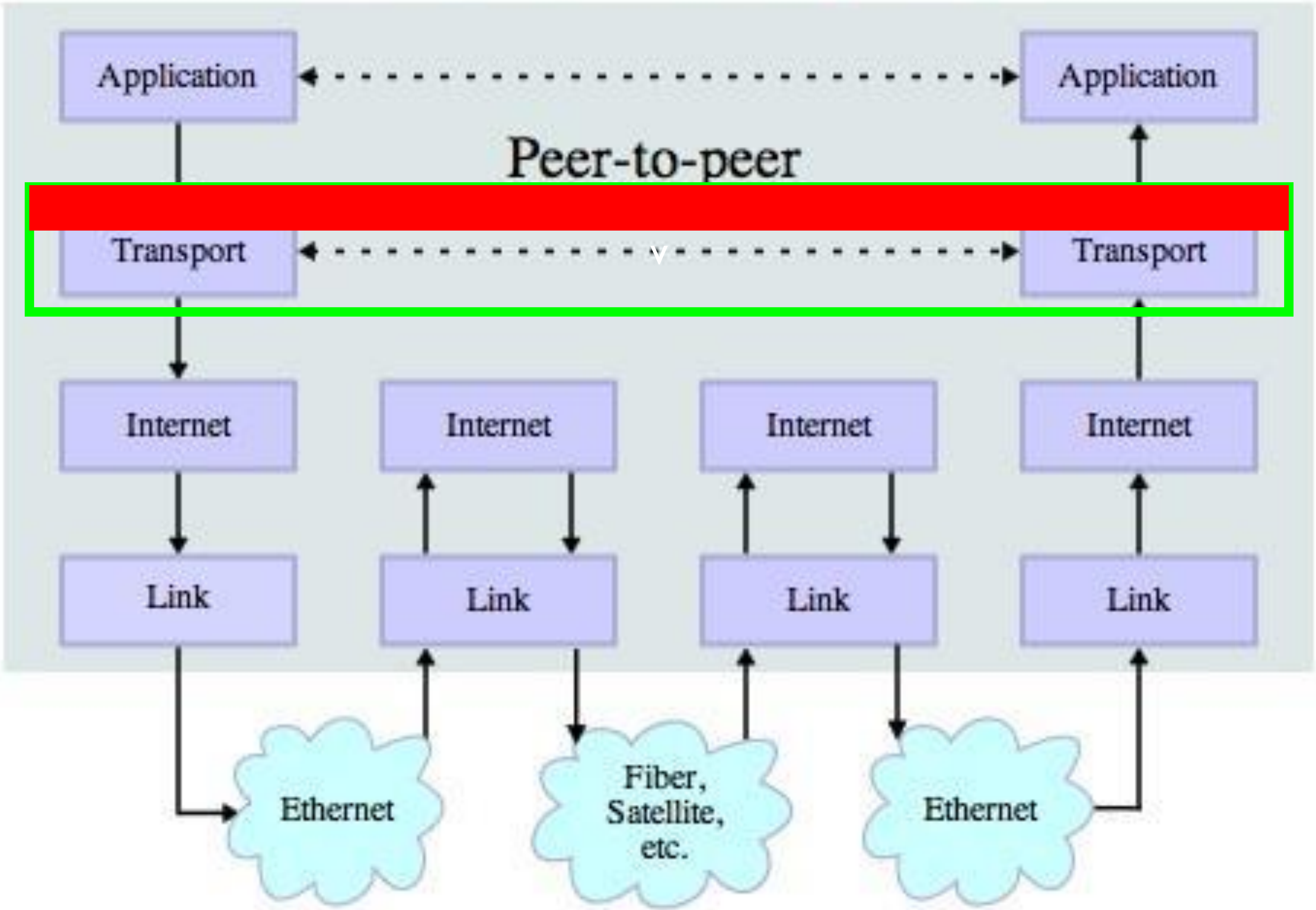
Your Laptop

Certificate Authority (CA)

A certificate authority is an entity that issues digital certificatesA 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

Reuse of these materials

- I intend for these materials to be reusable as open educational resources for those who would do so in a responsible manner

- Please contact me if you are interested in reusing or remixing these materials in your own teaching or educational context