Encryption 101

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
								Y				R					N	H	D						

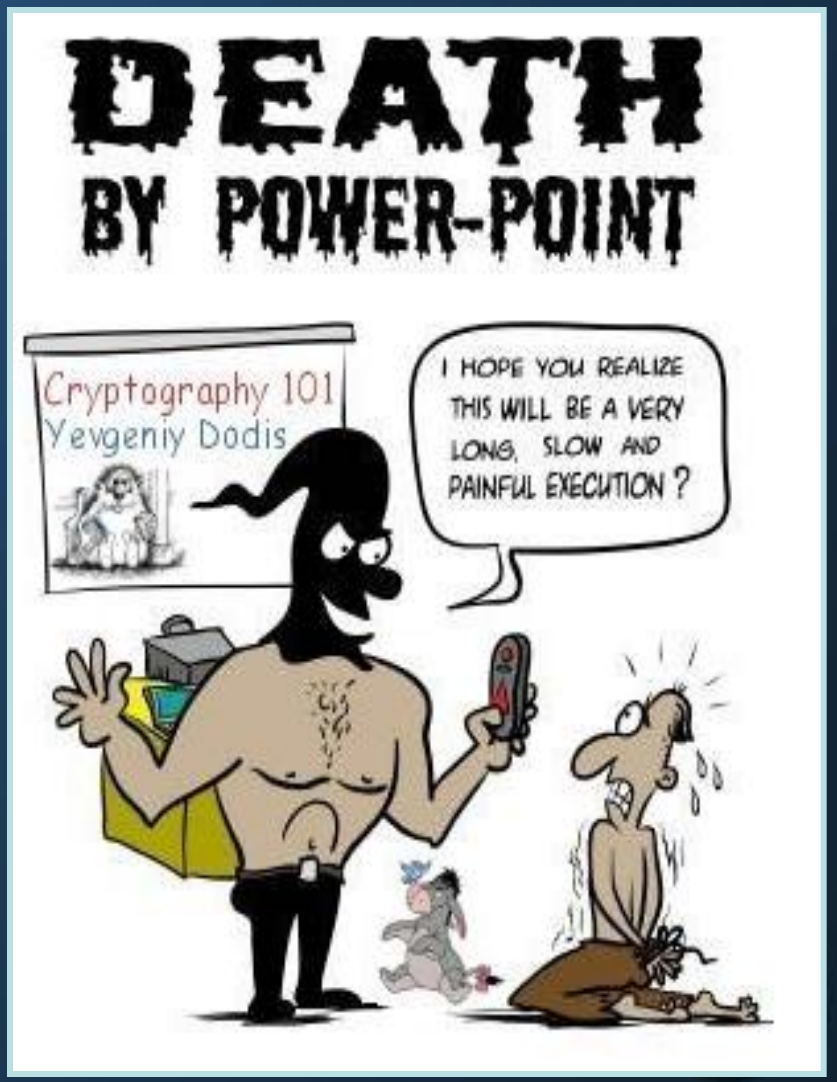
S _ _ _ R I T _ I S I M _ _ R T _ _ T

H O Q J N Y D G Y H Y R S T N D E K D

Information Security and Privacy Office

Agenda

- Review
  - CIA, trust, and non-repudiation
- Types of encryption
  - Symmetric
  - Asymmetric – public key
  - Hash – one-time pads
- Encryption in real life
  - Digital certificates
  - VPN
- Encryption for personal use



Definition – Info Security

- Protecting info and information systems from unauthorized
  - Access
  - Use
  - Disclosure
  - Disruption
  - Modification, or
  - Destruction

Confidentiality

- Confidentiality prevents the unauthorized accidental or malicious use or disclosure of information

EPA security breach exposes personal information of 8,000 people

Washington Business Journal by Jill R. Aitoro, Senior Staff Reporter
Date: Thursday, August 2, 2012, 10:14am EDT - Last Modified: Thursday, August 2, 2012, 10:44am EDT

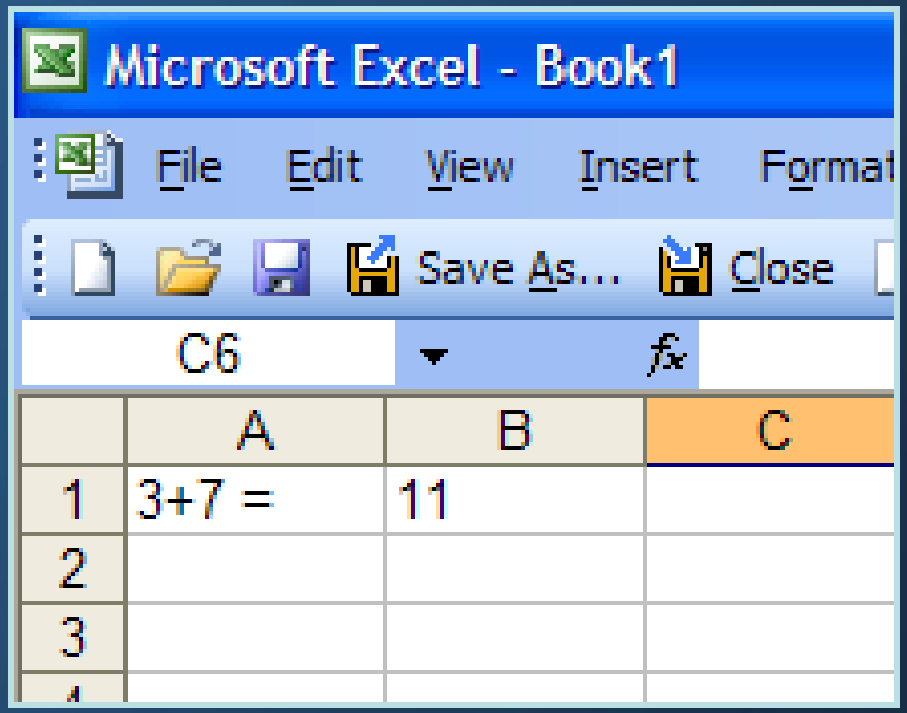
Data breach costs LinkedIn up to $1 million

By Marcos Colon on Aug 6, 2012 3:36 PM
Filed under Risk

LinkedIn's 2Q earnings call reveals that the company spent between $500,000 to $1 million on forensic work surrounding a recent data compromise.

Integrity

- Integrity safeguards the accuracy and completeness of information

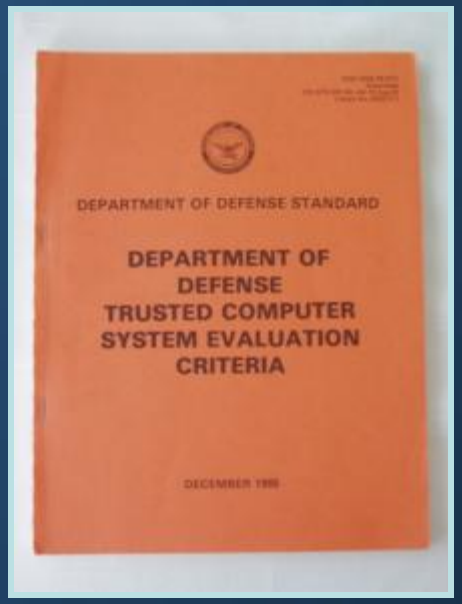


Availability

- Availability ensures that authorized users have reliable and timely access to information and computer systems when required

Trust

- Trust is when you have confidence in a system
  - Examples:
    - System X actually is System X
    - System X has appropriate security policies
- Trust is vital for internet communications and commerce

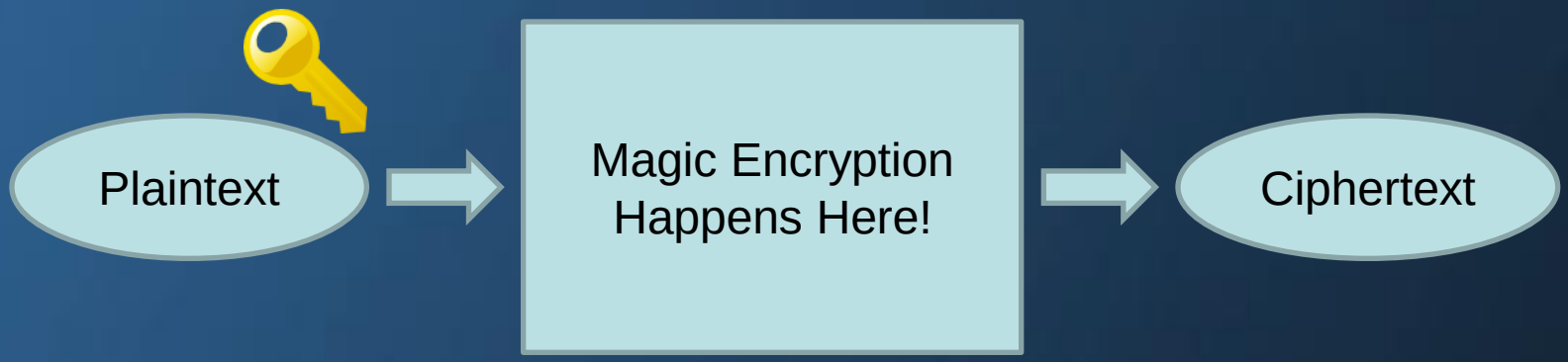


Non-Repudiation

- Non-repudiation is when the “data owner” can’t challenge that something isn’t valid
  - Examples:
    - Jim sent the email
    - Jim signed the contract
    - Document hasn’t been modified
  - So you can’t say it wasn’t you who ordered 10,000 pairs of Bright Feet

Encryption

- The practice of obscuring the meaning of a piece of information



Example: Encrypted Data (Ciphertext)

LÁüS§ •ŒØû ñC¾Moh û(Ï E6½j .8Ö!£B¤U‰ Œê´~Rz ü•ù}ÆeÿÊ4äQ™-
¯¼vw´4òbÕKŒÖJ • ?s +¨ÍÈn Ø×Ä±ÂóyQŸ X“Î^Ï¡{/soK $æ/š ¿ ➔◥
e~ù`.ºÐå¸¹Nãjuo ª ÞGb O?‰{;B$°ƒÂbLžW2 ý p`#y ˜²)}“ß¼PÃZ§□áÞ„’
ÓÈ7H¬ïÊVÁ_Z ?¬×--fOð w•âÀœ{'Oý ‡¥|G_ÂËz ªË§ˆG¡«þXŽ¥€… N ÉŒõ
ÖqHFIlã›Ï/b ›†ZB 'Ö2??i?Ä\ ÷"bÔûy¦KÎKMjÆ•Gõ³°¤Ts¼F,÷‹#% jÑ®?
0RqBý5ƒÉžÿØ,^—ù7ÁÑ44hµŸ ¦ û¥®§ÎNw/+6k4 R1ïŠ× š^^K£¥l‘wRÀ¹Ty…
Oª™ÑÛÐØ ´H£±≠\ÙÝ¥yDòªV:\}’8ïÓaéB !ž™‘¨ƒ´½…'y+6ž— Ó[”?w µžŒç-
È}u ›•mÀEÞ|F«½5"£ÙÖ më¬ms vÑ 4 Éó97b6v 4U[|ql!@ "a,8Ãµ ú»´q[zÅ’
Wou^QµÞ8ëdmœÜŸÜ8;0 ïa / ^›ï[Ž¥M<ül=±N}À N`üüô×Ý0•1¦Rú?W€lÜ7/‡
Ÿ€’^#1„ xö3À ª F ø ž¨H J5=öƒô‹˜ê7Nêv‰,× õT‘HGµ«è OLÕw -gO{[ê %
ÅõŒñp{íÁ<†:ôgÒ b-Td7â95‡Õ ! ËòlµÇ¿¬°□r"ÔT9 (OR ¶Ï ™ÉO4#8Âí
Þñ?ºA~OiÁ¾ZQ‘î2¥ä&Äs? (ŸÌ\Ç;0€öH÷sZ67ÕfŠ£8ý¼r—áX÷Hñ¹âá
𝔼⇆↙Q‡ºã?°#(šxÙ8€<¸ ë¡þ"ù•ä¬w Åj\õ£¢ùéb> Q «D Â3s Ó)Nný¹aÄ6"+?^.f
o†û ? ;3*j)%!!! ÷lJИ Jd^R‰ðsÿäc t¾ž?Ž ›’¾ l=Ä^!¤ m èkÕü±%Kdf1Í°T ô
nN½žG s.jûü½/zÚws_ZãÊðÓÐµRM]L [l„Gò•©Í½i¾÷³ ™Í •þP)/Î

True or False

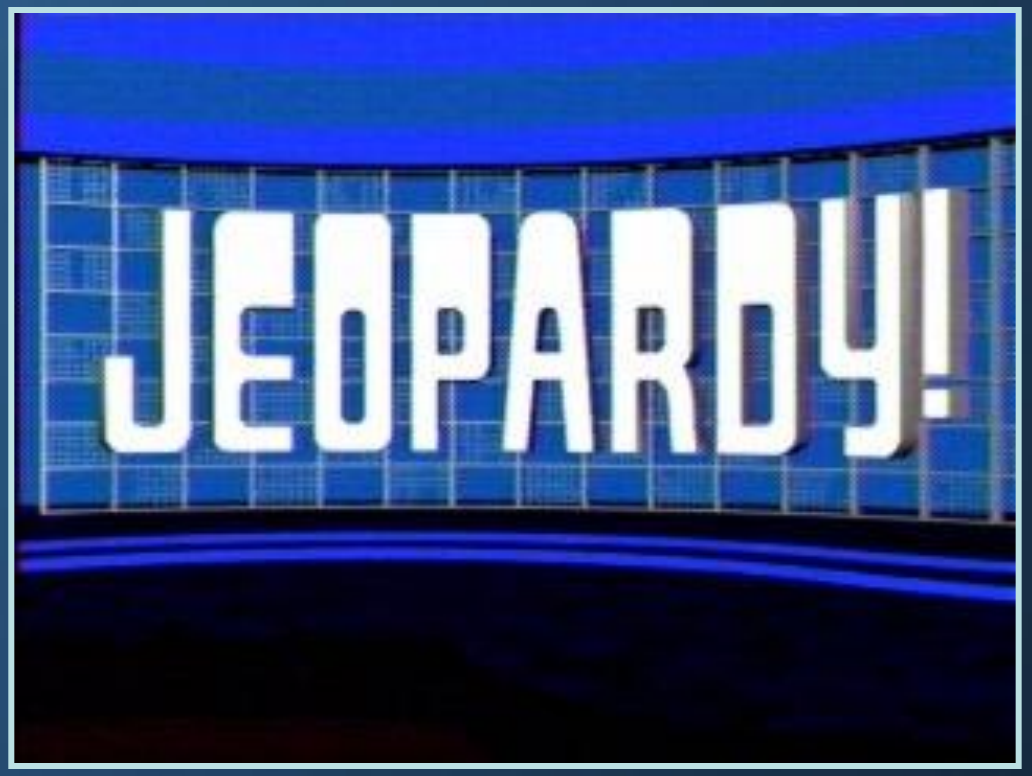
- If we have a breach of PII we must notify affected individuals

True or False

- If we have a breach of PII we must notify affected individuals

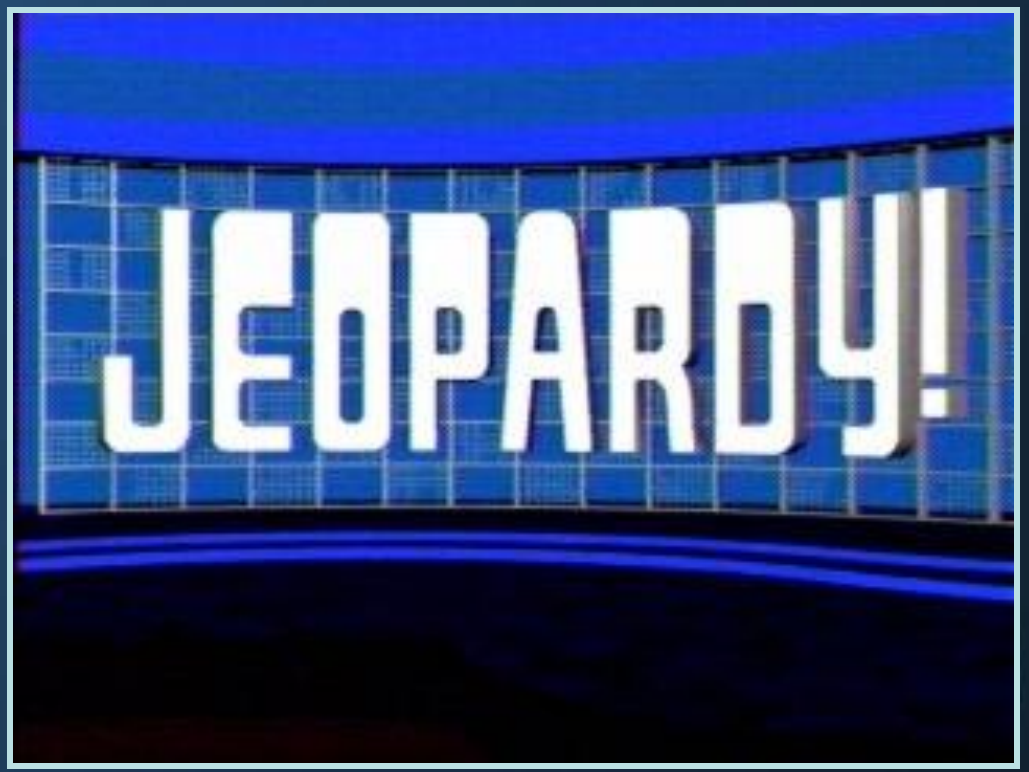
Breach Notification Jeopardy

- This is when you do not have to notify individuals' their PII was breached



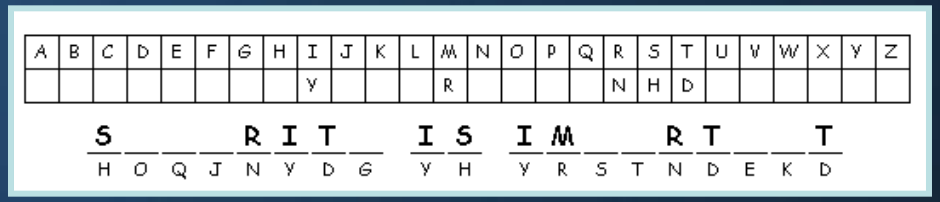
Breach Notification Jeopardy

- What is when the PII was encrypted
  - When you do not have to notify individuals their PII was breached



Encryption System Techniques

- Transposition
  - Rearranges characters
    - Example: secret → terces
- Substitution
  - Replaces characters with other characters



- Confusion
  - Makes the relationship between the plaintext and ciphertext as complex as possible
    - Example: HAL → IBM (1 letter difference = no confusion)
- Diffusion
  - Spreads the change throughout the ciphertext
    - So if one bit of the plaintext is changed, then the ciphertext should change completely

Encryption Is Based on Math

- Plaintext passes through a series of mathematical operations (an algorithm)

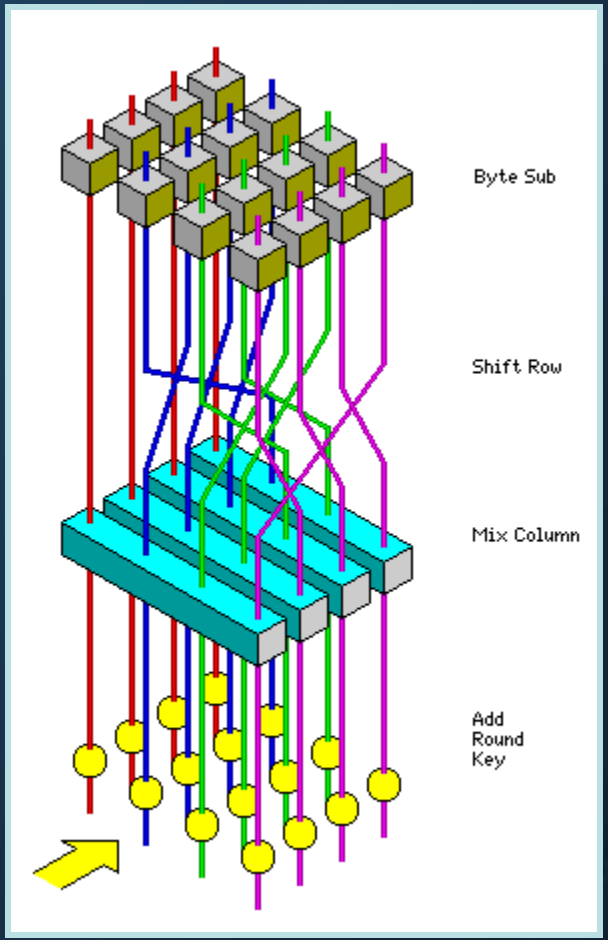
- Example: AES (aka Rijndael)

To encipher a block of data in Rijndael, you first perform an Add Round Key step (XORing a subkey with the block) by itself, the regular rounds noted above, and as already noted, the final round with the Mix Column step, as described below, omitted.

The Rounds

Each regular round involves four steps. First is the **Byte Sub** step, where each byte of the block is replaced by its substitute in an S-box.

The specification for Rijndael only provided an explanation of how the S-box was calculated: the first step was to replace each byte with its reciprocal in the same GF(2^8) as used below in the Mix Column step, except that 0, which has no reciprocal, is replaced by itself (since it isn't anything's reciprocal either, it is the only value not used, so that makes sense) then a bitwise modulo-two matrix multiply was used, and finally the hexadecimal number 63 is XORed with the result. (Not C6, x7 is the MSB, if the diagram in the specification appears confusing.)



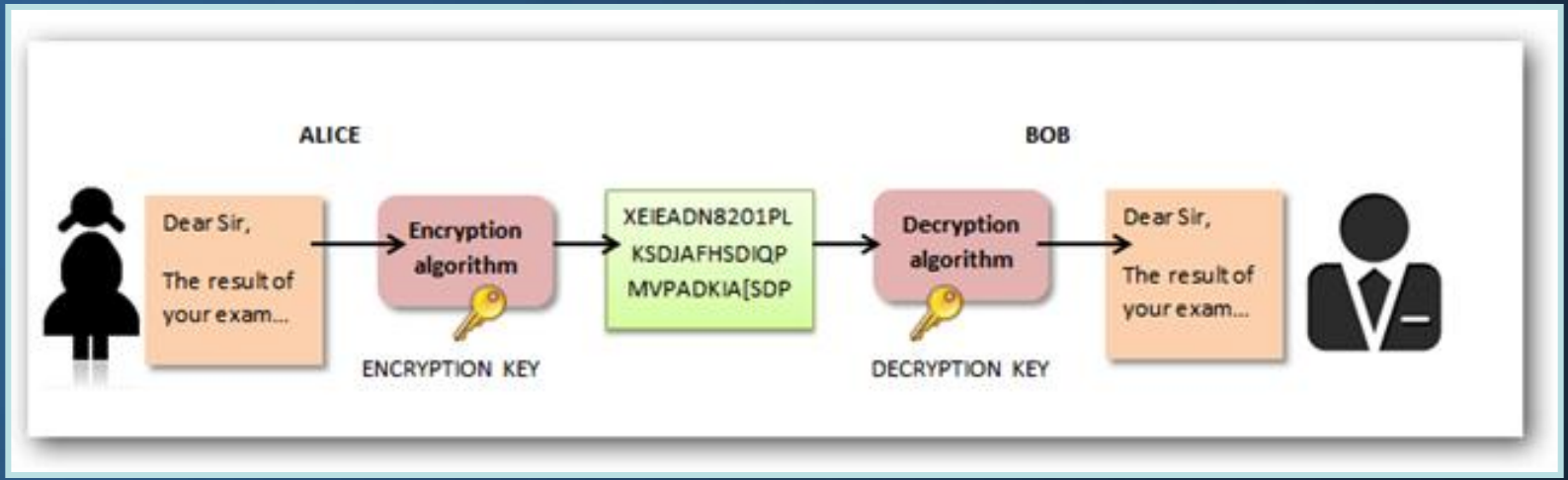
Types of Encryption

- Secret / private key
  - Symmetric
- Public key
  - Asymmetic
- Hash
  - One way transformation (can’t decrypt it)

Symmetric Key Encryption aka Private Key

- Alice and Bob share the same key

- Use the same key to encrypt and decrypt



About Symmetric Key Encryption

- Very fast
- Strength of cryptosystem based on algorithm and key length
- Common algorithms: AES, Blowfish, DES, Triple DES, Serpent, Twofish

- Problem: How do you securely distribute the key?
  - The more folks who have the key, the weaker the system

Asymmetric Encryption aka Public Key Encryption

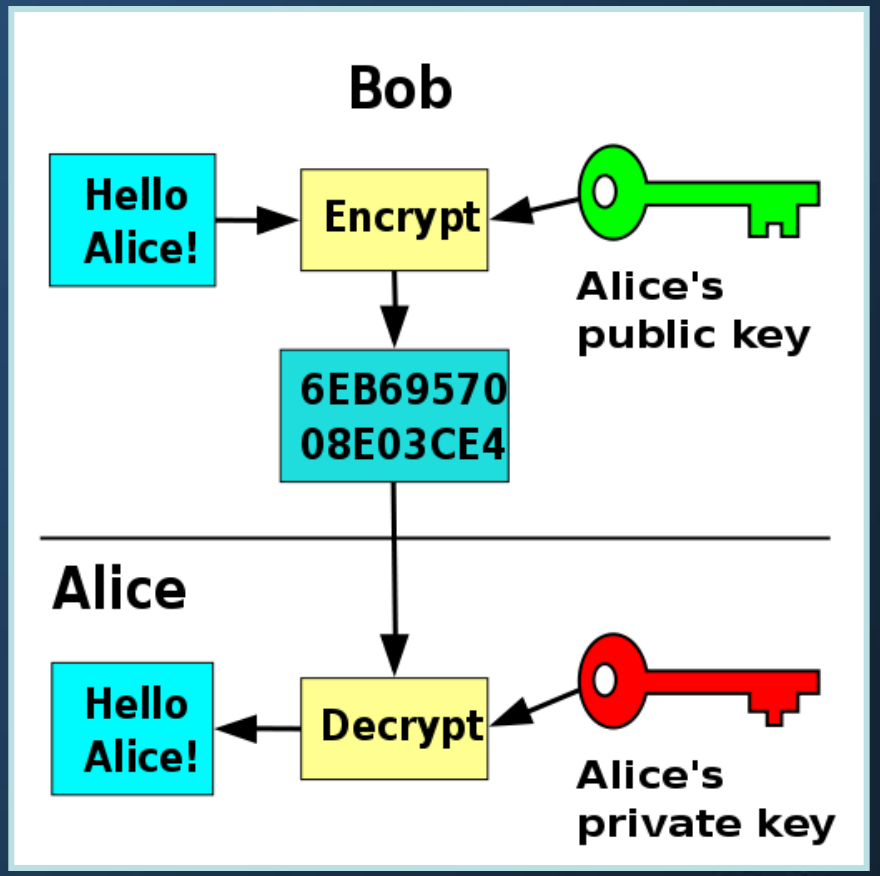
- Algorithm generates 2 linked keys
  - Public and private
- Any text encrypted with private key can only be decrypted with public key
- Any text encrypted with public key can only be decrypted with private key
- You cannot encrypt and decrypt with the same key

Public-Key Encryption Analogy

- Public-key encryption is like a locked mailbox with a mail slot
- The mail slot is exposed and accessible to the public
- Its location (the street address) is basically the public key
- Anyone knowing the street address can go to the door and drop a written message through the slot
- Only the person with the (private) key can open the mailbox and read the message

Public Key Encryption

- I keep my private key and distribute my public key
- You use my public key to encrypt a message for me
  - Only I can decrypt message using my private key



About Public Key Encryption

- Slow
  - Encrypts kilobits/second vs. symmetric's megabits/second
- Strength of cryptosystem based on algorithm and key length
- Examples of algorithms: RSA, El Gamal
- Examples of protocols using public key algorithms: PGP, Secure Socket Layer (SSL), Secure Shell (SSH), Bitcoin

- Overcomes issues with securely distributing the key
  - You're not sharing a secret (the key)

Mix and Match

- Symmetric key is fast, but I can't get you my key
- Public key is slow, but I can get you my key

- Combine them
  - Use public key encryption to distribute symmetric keys!

True or False

- I would never encrypt a message with my private key – there's no reason to

Reminder

- You encrypt messages to me with my public key
- I decrypt them with my private key
- This assures confidentiality

Follow-Up Question

- If I encrypt a message with my private key, who can decrypt it?

Follow-Up Question

- If I encrypt a message with my private key, who can decrypt it?

- Anybody with my public key

I would never encrypt a message with my private key – True or False

- Encrypting a message with my private key proves that I sent the message
  - Assures non-repudiation

- ** Technically, I wouldn't encrypt the message; I would cryptographically sign it using a signature algorithm

Pop Quiz Pictorial (kinda)

Ilene's private key

Encrypting with my private key proves I sent it
Anybody with my public key can decrypt and read it

Only I can read mail encrypted with my public key

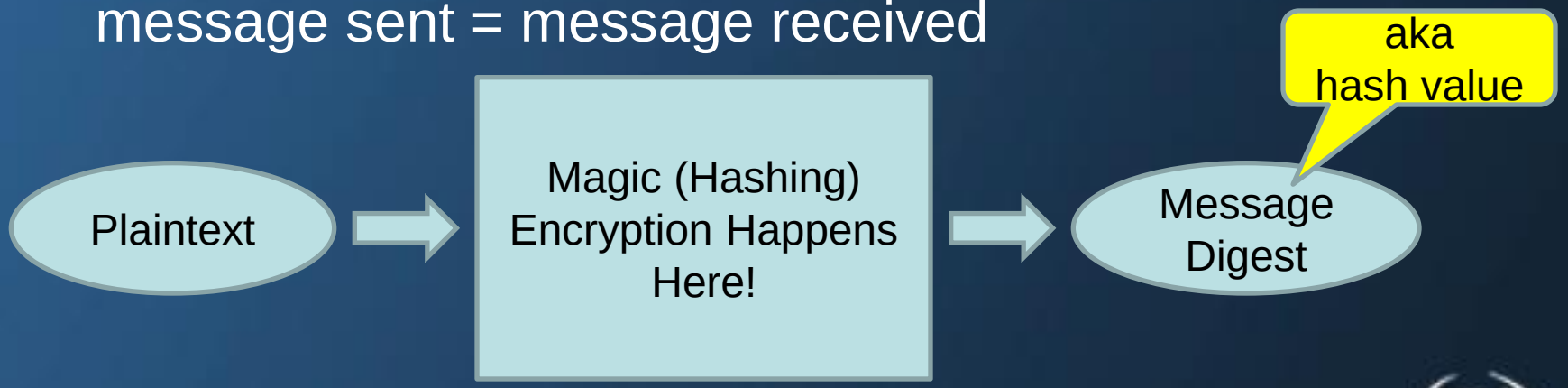
Ilene's public key

Ilene's public key

Ilene's public key

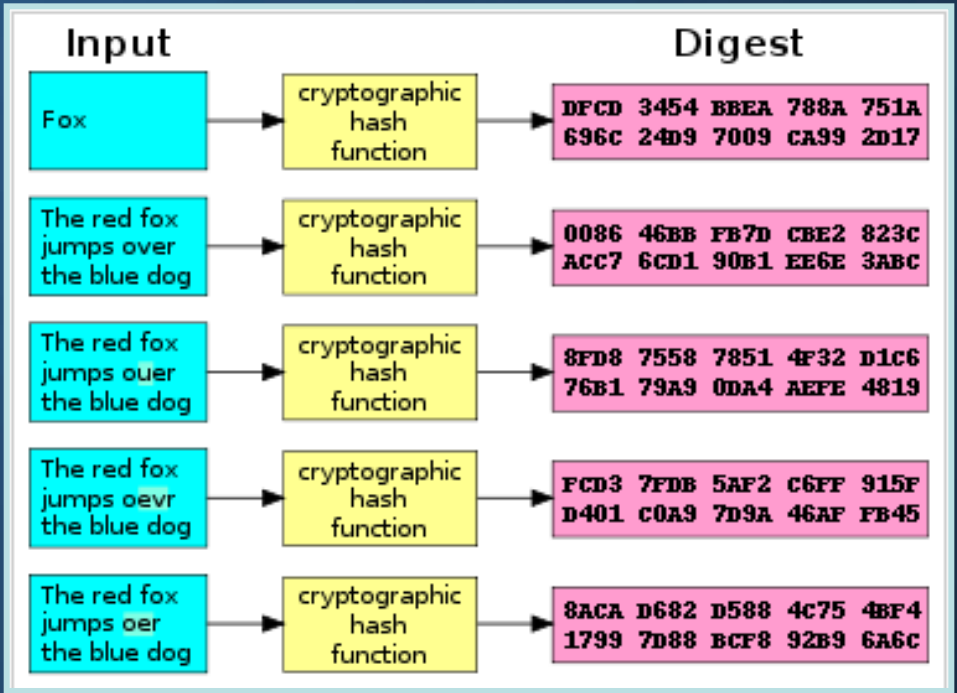
Hash Function

- One-way encryption – can't decrypt
  - Has no key
  - Hashing creates a fixed length message digest
- Primary use is for message integrity
  - By comparing hash values, you can see if message sent = message received



Why Hash? Integrity

- You change one little letter and the entire hash value changes
  - Example of diffusion
    - Spreads the change throughout the ciphertext



Why Hash?
Keep Original Data Confidential

- Passwords are commonly hashed

- Password files actually contain hash of your password – not the password itself
  - When you log in, the computer hashes your password and compares the hash value to the hash value of the password that's on file

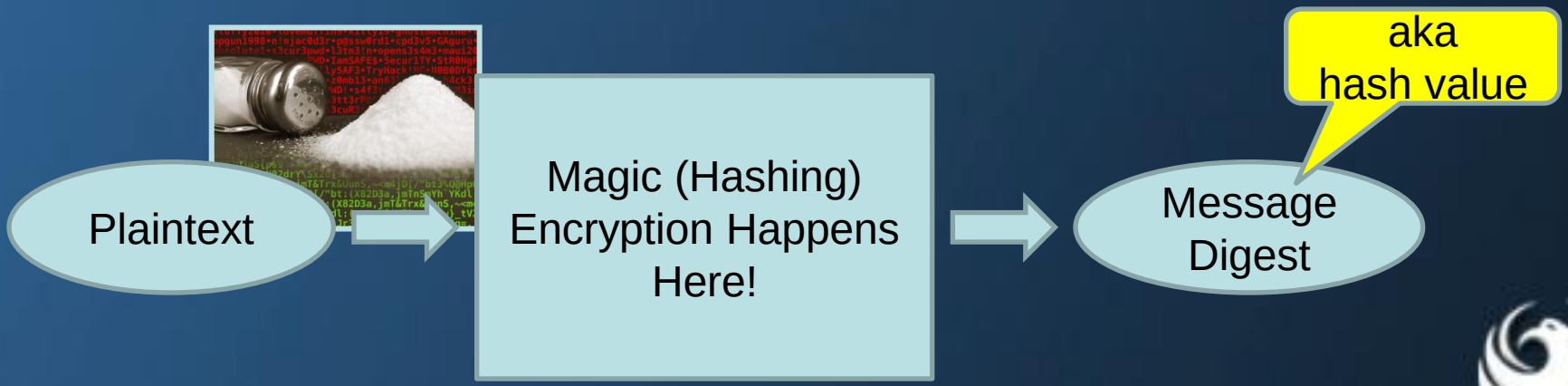
So How Do Hackers Crack Passwords?

- Brute force – try every combination of characters
  - Slow and requires a lot of computing power

- Use tables of pre-hashed passwords (called rainbow tables)
  - Use a hash algorithm and hash words in a dictionary and the 500 top passwords
  - Steal a password file and just compare the file (hashed passwords) to the list (hashed words)

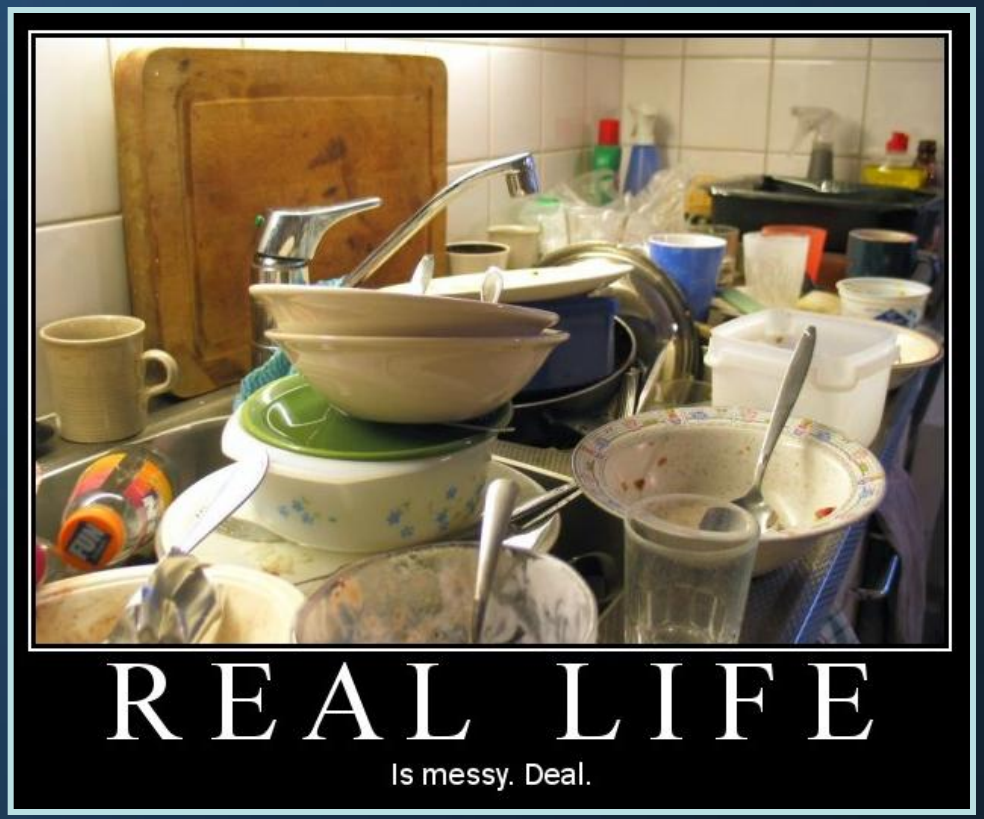
Defend Against Password Hackers: Salted Hash

- Salting adds a string of random characters to the passwords before they are hashed, so that each one has a unique hash
  - Hacker has to crack every user's password individually, even if there are a lot of duplicate passwords



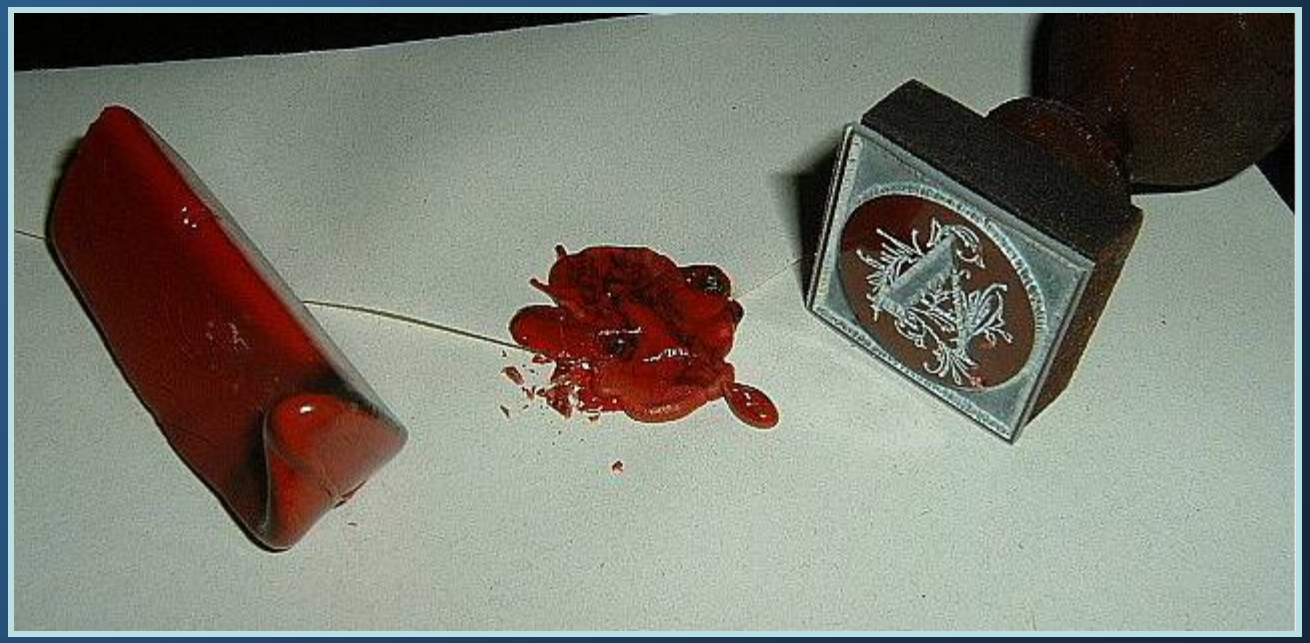
Encryption in Real Life

- Digital signatures
- VPNs
- Digital certificates
- Electronic commerce



Digital Signature Analogy

- Sealing an envelope with a personal wax seal
  - The message can be opened by anyone, but the presence of the unique seal authenticates the sender
    - Private key acts like the wax seal (in this context)

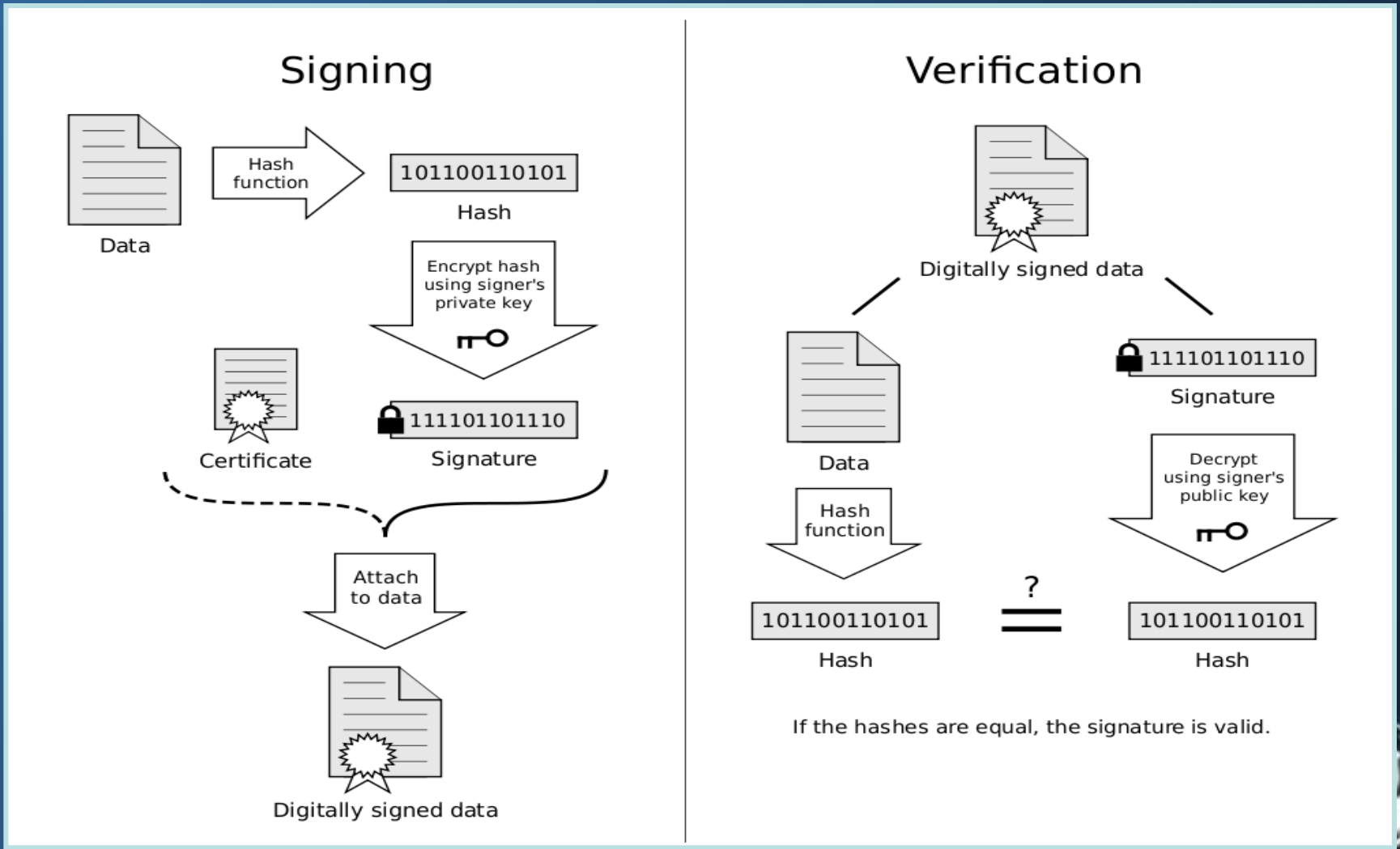


Digital Signatures and Hashes

- A digital signature is a hash value that has been encrypted with the sender's private key

- A message can be
  - Encrypted, which provides confidentiality
  - Hashed, which provides integrity
  - Digitally signed, which provides authentication, non-repudiation, and integrity
  - Encrypted and digitally signed, which provides confidentiality, authentication, non-repudiation, and integrity

Digital Signatures



VPN – Virtual Private Network

- A “tunnel” through the internet
  - IPSec = IP Security protocol
    - A suite of protocols providing a mechanism to provide data integrity, authentication, privacy, and nonrepudiation for the classic Internet Protocol (IP)
    - Puts a “wrapper” around your message to keep it secure

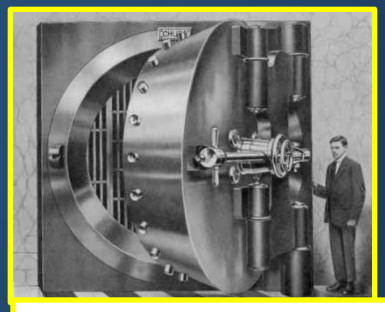
SSL – Secure Sockets Layer

- Protocol developed by Netscape to secure communications over the Internet for protocols such as the Hypertext Transfer Protocol (HTTP)
- SSL uses public key crypto and digital certificates during an initial handshake used to authenticate the server
  - The client and server then agree upon an encryption scheme
- SSL – the security protocol for the Internet

What's a Digital Certificate?

- Digital certificate: Electronic document to verify that users and websites are who/what they claim to be
  - Often used in email to verify sender
  - Used on websites to indicate they're authentic

My credentials



Are verified by a certificate authority

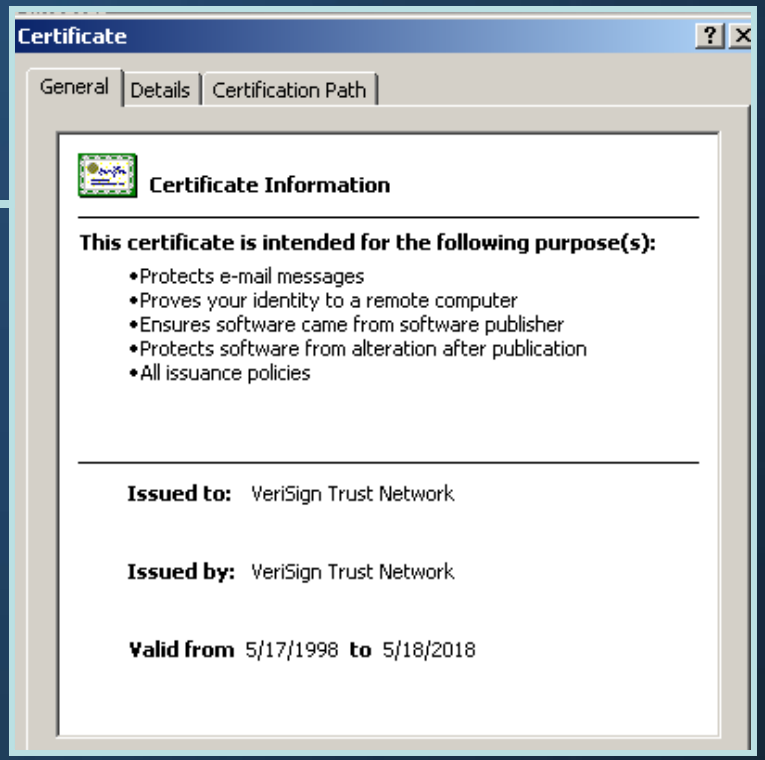
That issues a digital certificate

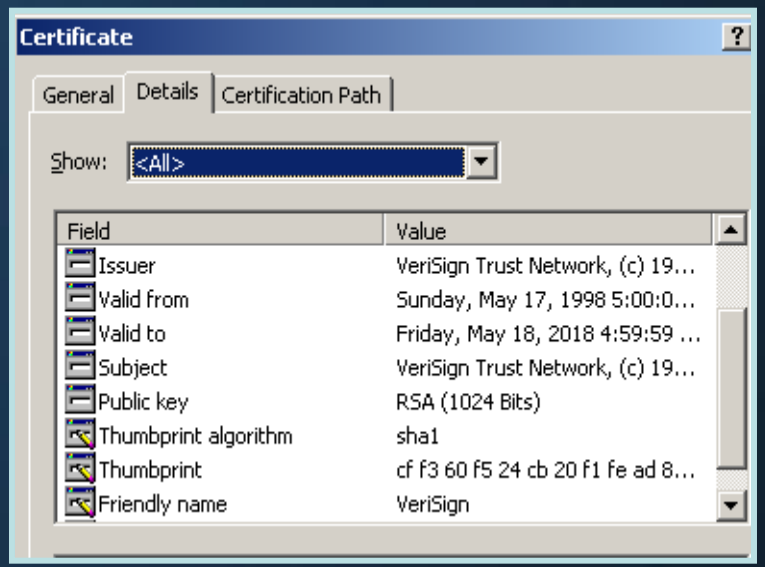
More on Certificates

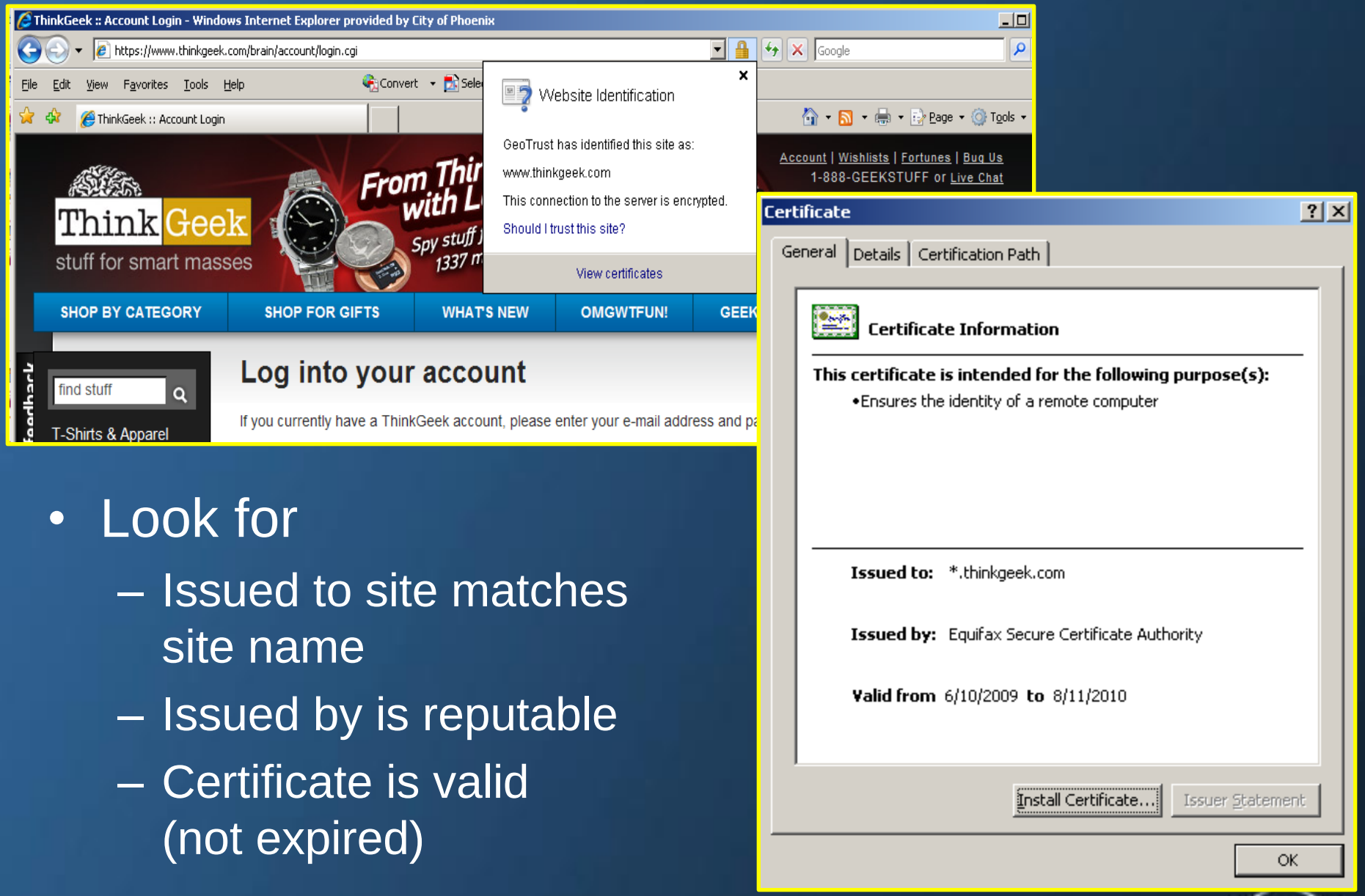
- X.509 is the standard
- Certificates usually contain a public key, a name, an expiration date, the name of the authority that issued the certificate (and, therefore, is vouching for the identity of the user), a serial number, any pertinent policies describing how the certificate was issued and/or how the certificate may be used, the digital signature of the certificate issuer, and perhaps other information
- For purposes of electronic transactions, certificates are digital documents used to
  - *Establish identity:* Associate, or *bind*, a public key to an individual, organization, corporate position, or other entity
  - *Assign authority:* Establish what actions the holder may or may not take based upon this certificate
  - *Secure confidential information* (encrypting the session's symmetric key for data confidentiality)
- Browsers come with a bunch of certificates from known certificate authorities

Certificates Contain…

- Public key
- Name of person/site being authenticated
- Expiration date
- Name and digital signature of the certificate authority vouching for the user's identity
- Serial number
- Pertinent policies describing how the certificate was issued and/or how the certificate may be used

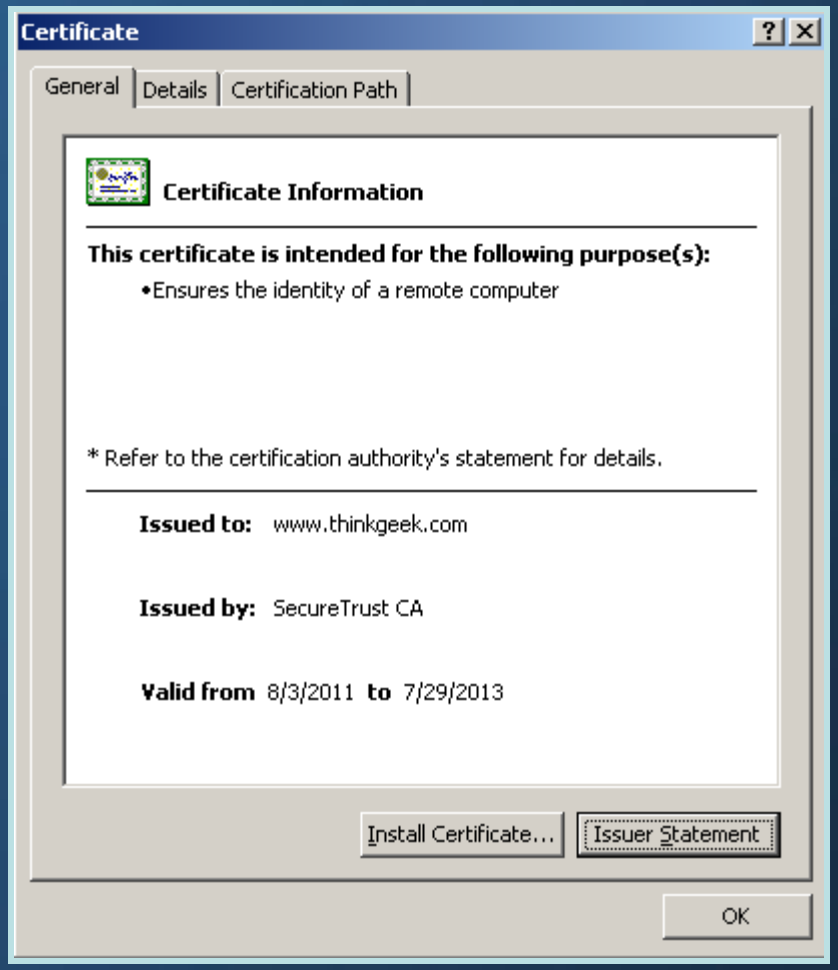




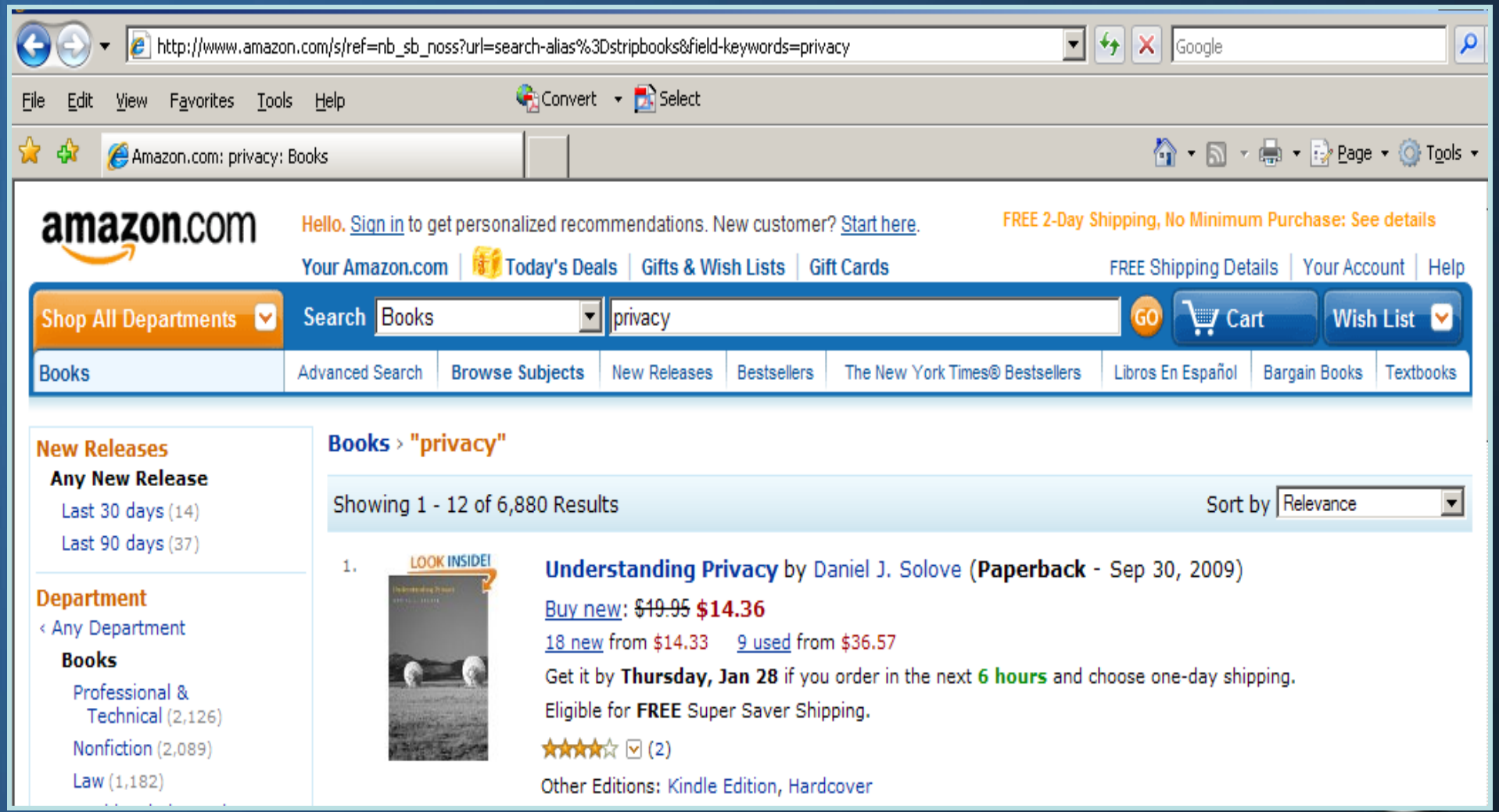


- Look for
  - Issued to site matches site name
  - Issued by is reputable
  - Certificate is valid (not expired)

ThinkGeek's New Certificate



SSL in Action:
http While Browsing Normally



SSL in Action: https During Login and Purchase

Pop Quiz

- Name two quick ways to determine whether you should trust a website

Pop Quiz
Should you trust a website?

- Check the protocol
  - Look for https:// in the address bar
  - “http” = normal; “https” = secure
- Check a site’s digital certificate
  - “Lock” icon in bottom right corner or by address bar

Biggest Problem with Certificates

- How do you manage certificates?
- You need a public key infrastructure (PKI)
  - Set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates
  - Very, very hard to do manually

Encryption for Personal (Not Office) Use

PGP – Pretty Good Privacy

- One of today's most widely used public key cryptography programs
- Used most often for email (personal)
- Create a key-pair when you first install PGP
  - Protect your private key with a strong passphrase
  - Distribute your public key
    - Usually via a public key server like http://pgp.mit.edu/ and https://keyserver.pgp.com

Example: PGP Signed message

- Sender encrypts message with private key
- Receiver

```
-----BEGIN PGP MESSAGE-----
Version: PGP for Personal Privacy 5.0
MessageID: DAdVB3wzpBr3YRunZwYvhK5gBKBXOb/m

qANQR1DBwU4D/TlT68XXuiUQCADfj2o4b4aFYBcWumA7hR1Wvz9rbv2BR6WbEUsy
ZBIEFtjyqCd96qF38sp9IQiJIKlNaZfx2GLRWikPZwchUXxB+AA5+lqsG/ELBvRa
c9XefaYpbbAZ6z6LkOQ+eE0XASe7aEEPfdxvZZT37dVyiyxuBBRYNLN8Bphdr2zv
z/9Ak4/OLnLiJRk05/2UNE5Z0a+3lcvITMmfGajvRhkXqocavPOKiin3hv7+Vx88
uLLem2/fQHZhGcQvkqZVqXx8SmNw5gzuvwjV1WHj9muDGBY0MkjiZIRI7azWnoU9
3KCnmpR60VO4rDRAS5uG19fioSvze+q8XqxubaNsgdKkoD+tB/4u4c4tznLfw1L2
YBS+dzFDw5desMFSo7JkecAS4NB9jAu9K+f7PTAsesCBNETDd49BTOFFTWWavAfE
gLYcPrcn4s3EriUgvL3OzPR4P1chNu6sa3ZJkTBbriDoA3VpnqG3hxqfNyOlqAka

mJJuQ53Ob9ThaFH8YcE/VqUFdw+bQtrAJ6NpjIxi/x0FfOInhC/bBw7pDLXBFNaX
HdlLQRPQdrmnWskKznOSarxq4GjpRTQo4hpCRJJ5aU7tZO9HPTZXFG6iRIT0wa47


AR5nvkEKoIAjW5HaDKiJriuWLdtN4OXecWvxFsjR32ebz76U8aLpAK87GZEyTzBx
dV+lH0hwyT/y1cZQ/E5USePP4oKWF4uqquPee1OPeFMBo4CvuGyhZXD/18Ft/53Y
WIebvdiCqsOoabK3jEfdGExce63zDI0=
=MpRf
-----END PGP MESSAGE-----
```

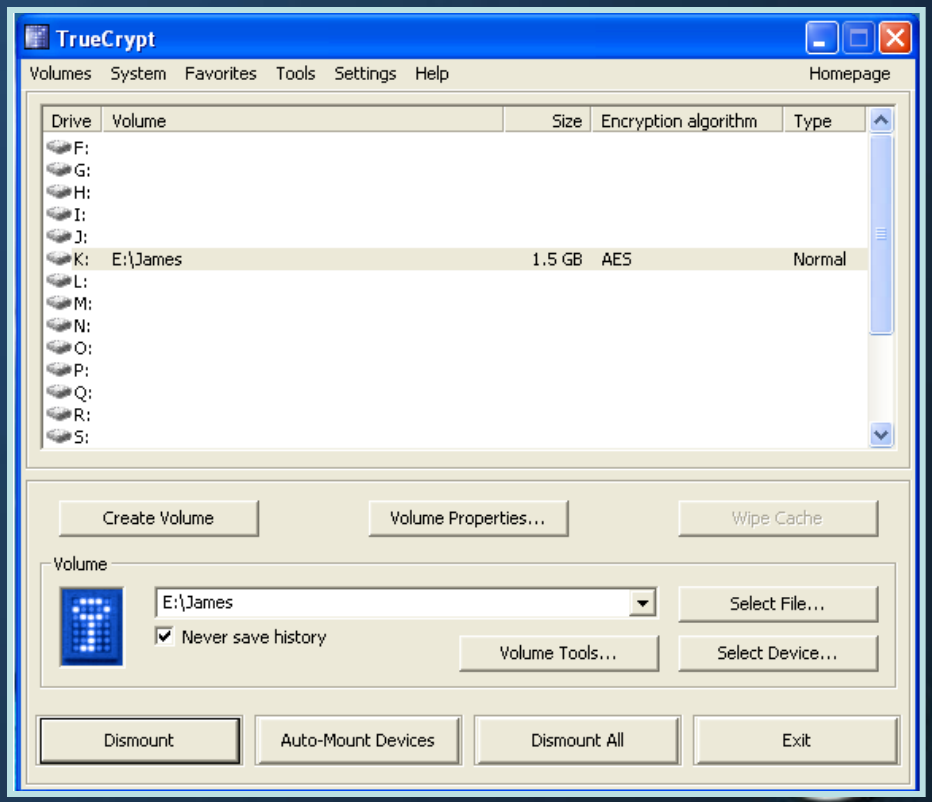
FIGURE 8: A PGP encrypted message. The receiver's e-mail address is the pointer to the public key in the sender's keyring. At the destination side, the receiver uses their own private key.

Wireless Encryption

- Use WPA2
- WEP and WPA are weak
  - Algorithms have been cracked
- You still must pick a strong passphrase

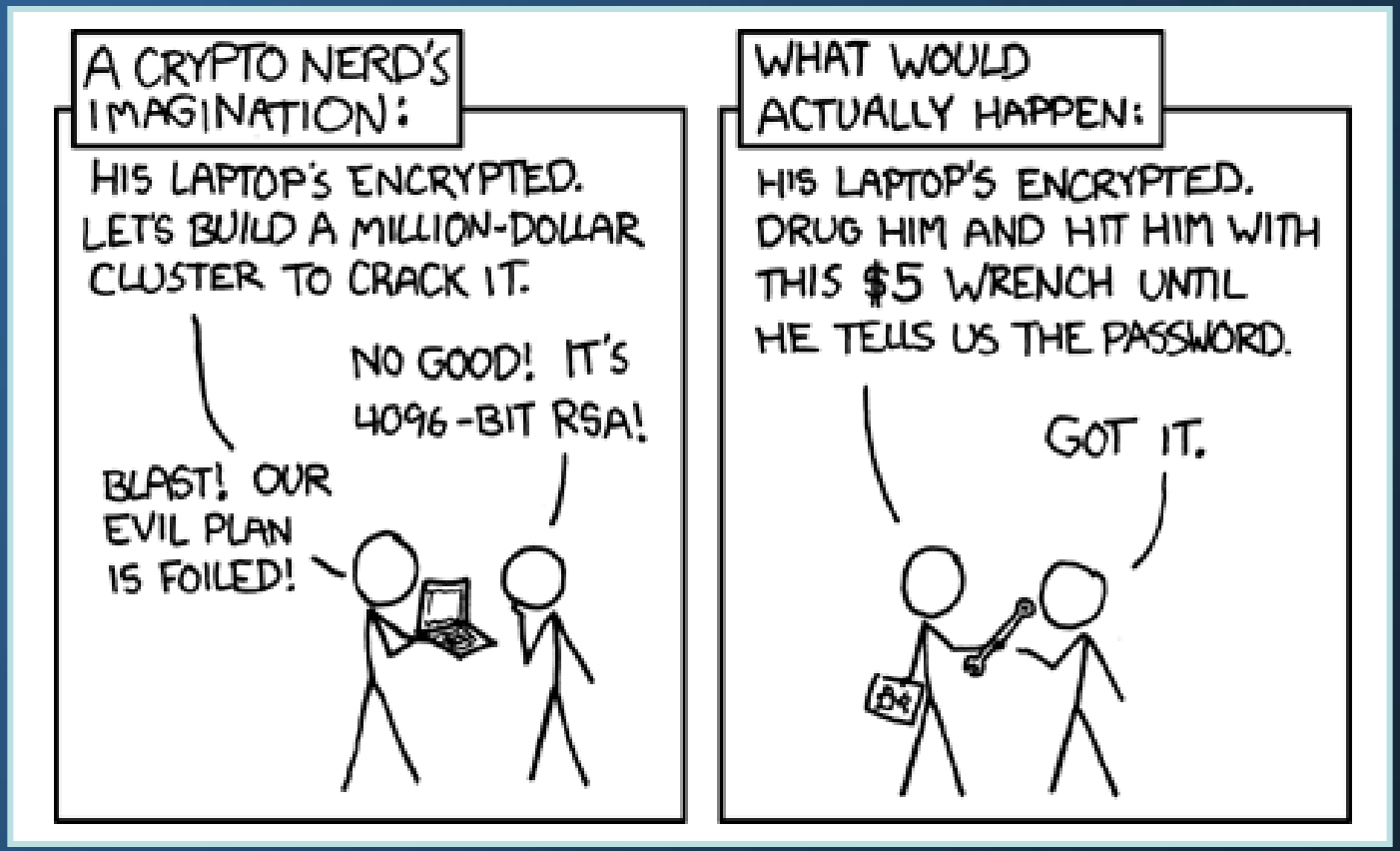
TrueCrypt

- TrueCrypt is an open source, on-the-fly crypto system used to encrypt a partition or an entire disk
  - Supported by Linux, Mac OS, and Windows
- Good for personal use
  - Hard to manage in an enterprise



Truth About Encryption

- Crypto does not solve all security problems



Encryption “Rules”

- Never, ever trust a “secret” or proprietary crypto algorithm
  - Unless developer works for NSA
  - Crypto algorithms must be peer reviewed
- Never, ever rely only on technology as your only wall of defense
- Above all, never, ever attempt to write your own encryption system
  - We’re not that smart (unless you worked for NSA)

True or False

- Encryption protects
  - Confidentiality
  - Integrity
  - Availability

True or False

- Encryption protects
  - Confidentiality **True**
    - Hides the original message
  - Integrity **True**
    - Proves that nobody messed with your message
  - Availability **False**
    - If you lose your encryption key, you lose your data

True or False

- If I encrypt my computer, I don’t need anti-virus software

- If I use anti-virus software, I don’t need to use encryption

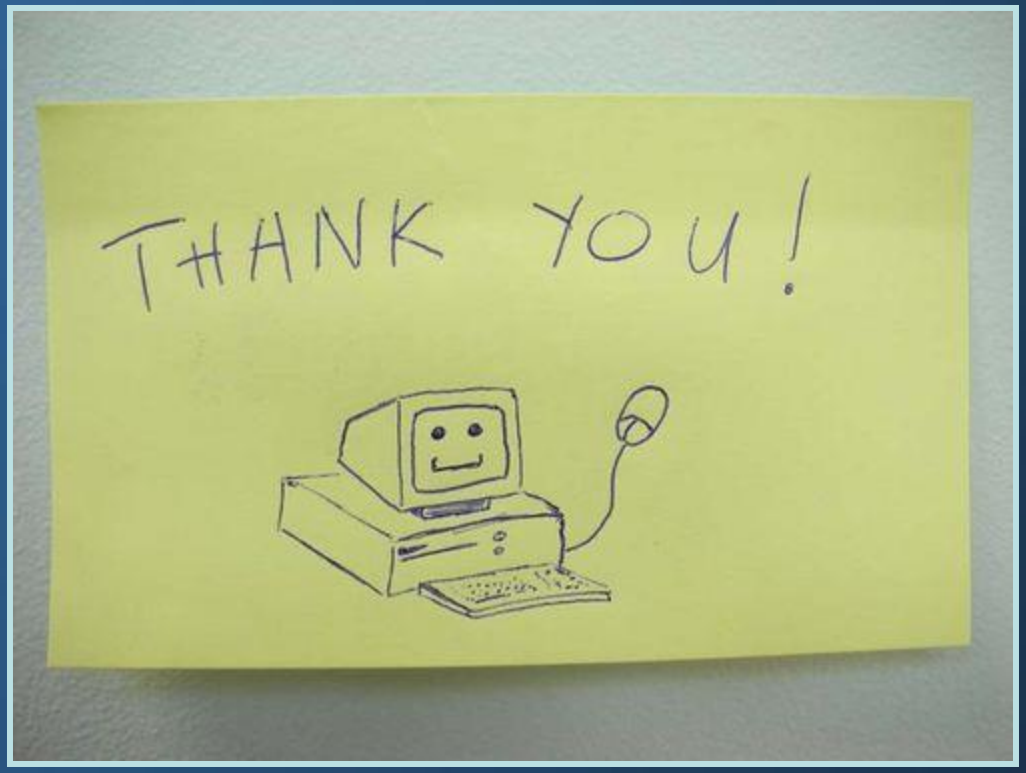
True or False

- In general, encryption does nothing to protect against viruses, worms, unpatched computers, social engineering…

- Encryption is another layer of security

Summary
Encryption Provides…

- Authentication
  - If Alice hands Bob a message, he knows for sure (trusts) the message came from Alice
- Confidentiality
  - Only Bob can see Alice's message
- Integrity
  - Can prove a message has not been tampered with
  - Bob receives the full and complete message from Alice
- Non-repudiation
  - Can prove that Alice, and only Alice, sent the message



Questions?
Contact ispo@phoenix.gov

More Cowbell
(Supplemental Info)

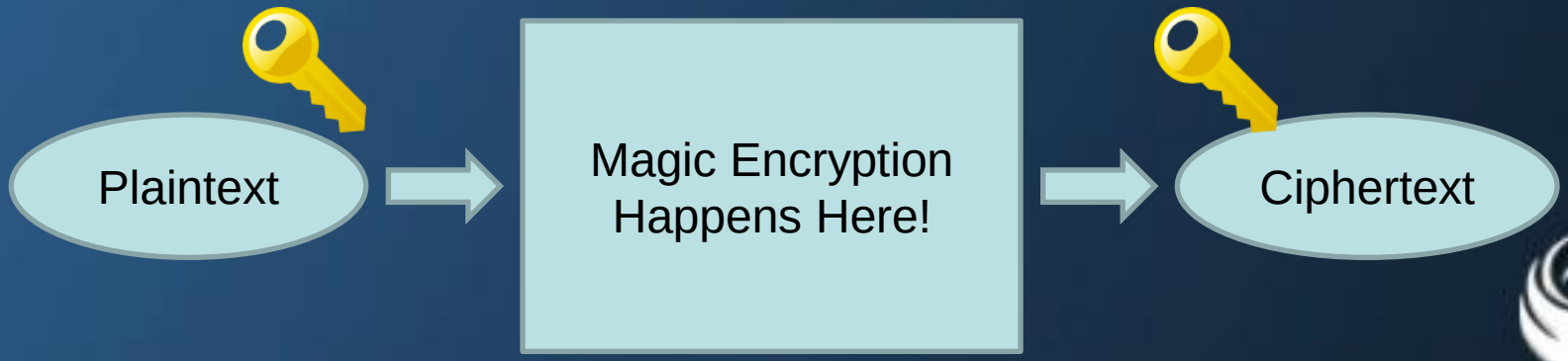
Why Encrypt?

- Main drivers for using encryption are
  - Compliance with privacy and data security regulations (65%)
  - Lessening the impact of data breaches (58%)
  - Protecting the company brand resulting from a data breach (43%)

    - 2011 Encryption Trends Study: United States, Ponemon Institute, 07/09/12

How Modern Encryption Works

- Most encryption is based on math
  - Computing the prime factors of very large numbers
    - Example: The number 15 factors into primes as 3 × 5
  - There is no known method to carry it out quickly
  - Its complexity is the basis of the assumed security of some cryptography algorithms



Steganography

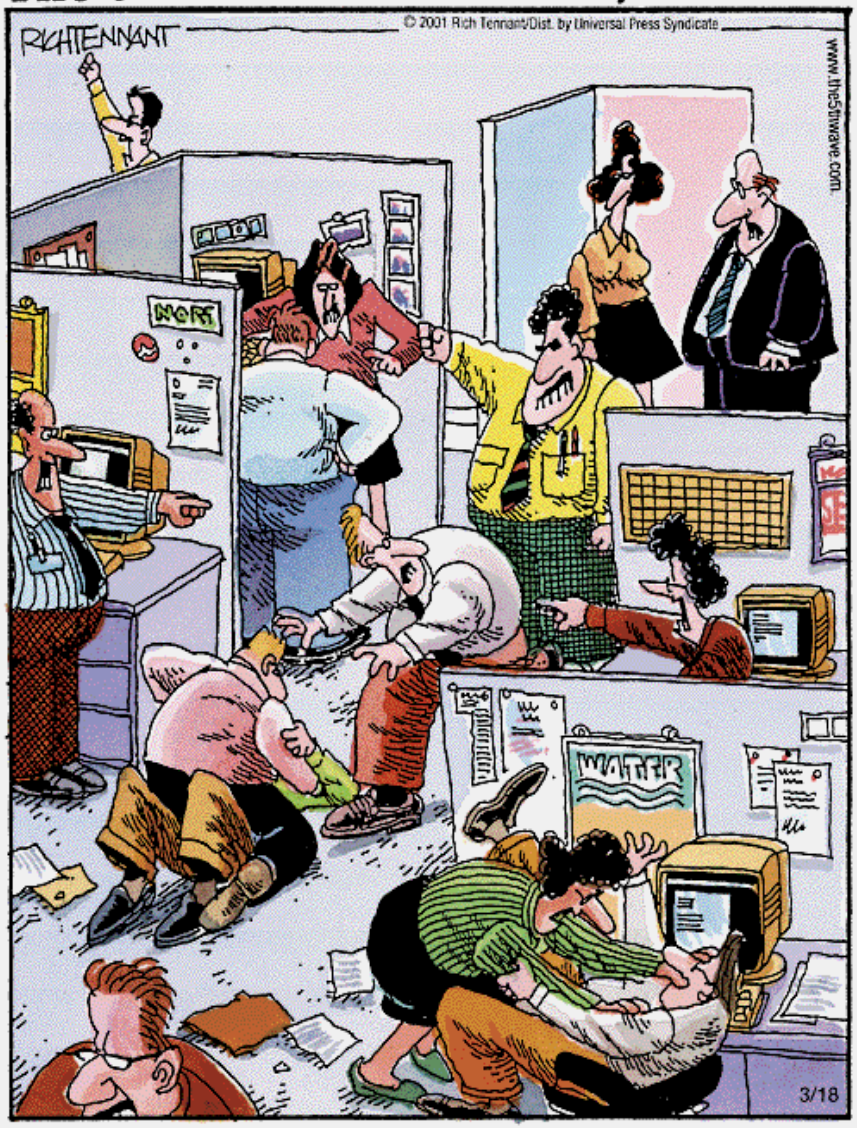
- Hiding messages in media files
  - Pictures
  - Sound
- Hides the fact that there's even a hidden message

- In binary, stego replaces the least significant bit with the message
  - Byte = 1001110**0**

5th wave.gif

The 5th Wave

By Rich Tennant

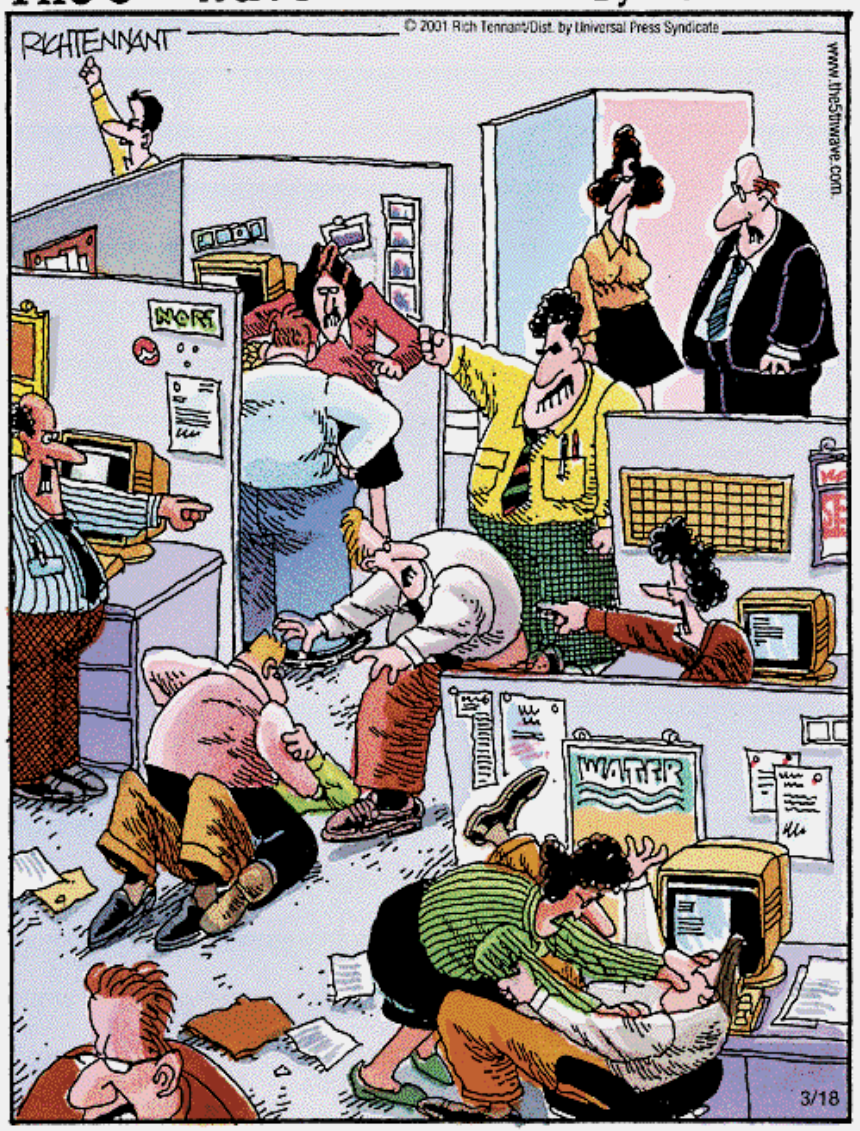


"Sure, at first it sounded great — an intuitive network adapter that helps people write memos by finishing their thoughts for them."

hidden data

The 5th Wave

By Rich Tennant



"Sure, at first it sounded great — an intuitive network adapter that helps people write memos by finishing their thoughts for them."

So how does SSL work?

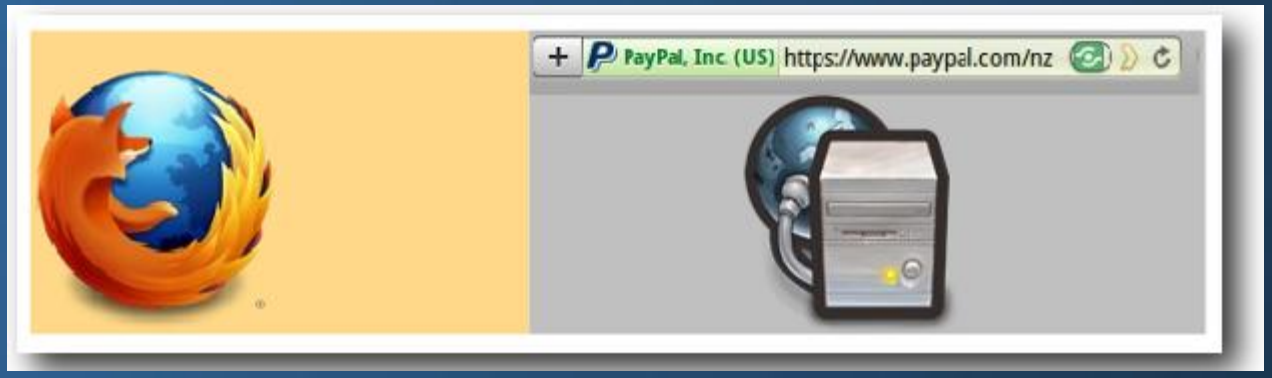
- During the SSL exchange with the vendor’s secure server, the server sends its certificate to our browser
- The certificate includes the vendor’s public key and a signature from the CA that issued the vendor's certificate
  - Our browser software comes with the major CAs’ certificates which contains their public key
- Note that the server does not use a certificate to authenticate us!
  - Instead, we are generally authenticated when we provide our credit card number
  - The server checks to see if the card purchase will be authorized by the credit card company and, if so, considers us valid and authenticated

What's that again?

- When the browser makes a connection to a secure Web site, the Web server sends its public key certificate to the browser
- The browser then checks the certificate's signature against the public key that it has stored
- If there's a match, the certificate is taken as valid and the Web site verified by this certificate is considered to be "trusted"

Secure Web Communications 1

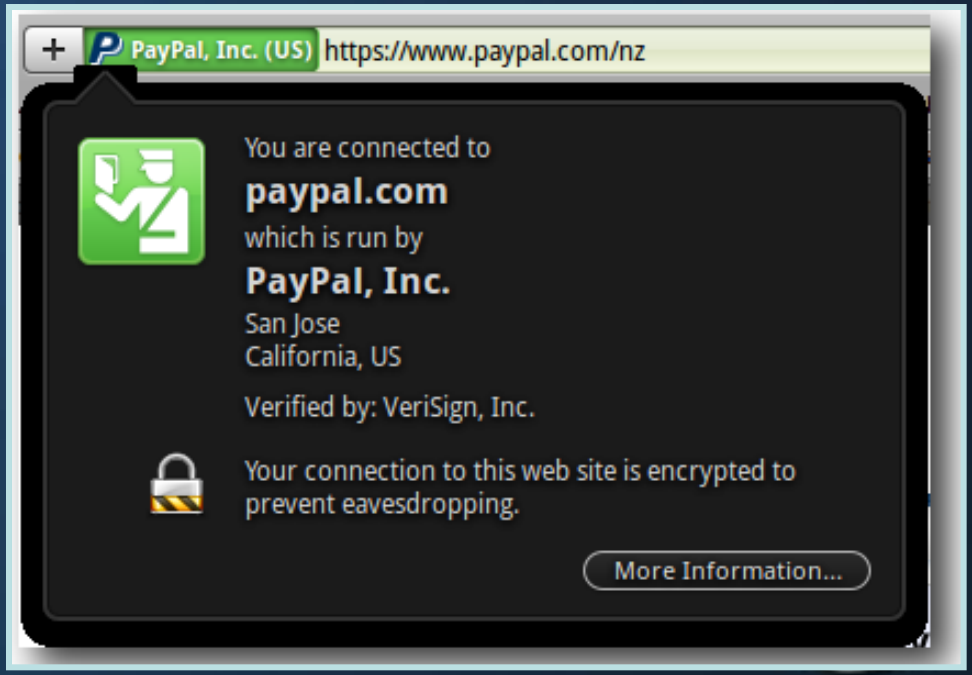
- Browser requests a secure page (https)



- Web server sends its public key with its certificate

Secure Web Communications 2

- Browser checks that…
  - Certificate was issued by a trusted party (usually a trusted Certificate Authority)
  - Certificate is still valid, and
  - Certificate is related to the site contacted
- If all is valid, browser trusts site



Secure Web Communications 3

- Browser then uses the public key to encrypt a random symmetric encryption key and sends it to the server with the encrypted URL required as well as other encrypted http data
- In other words, browser and website use this established trust and public key to securely exchange a symmetric key
  - Why? Symmetric encryption is faster

Secure Web Communications 4

- Web server decrypts the symmetric encryption key using its private key and uses the browser's symmetric key to decrypt its URL and http data

Secure Web Communications 5

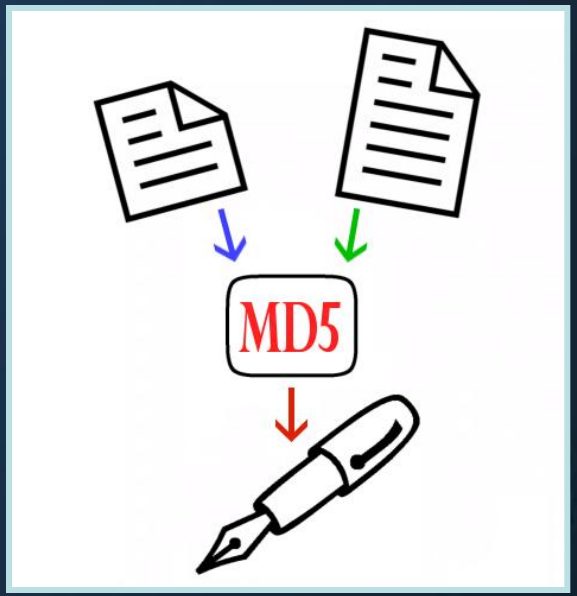
- Web server sends back the requested html document and http data encrypted with the browser's symmetric key
- Browser decrypts the http data and html document using the symmetric key and displays the information

Common Hash Algorithms

- MD5 – Message Digest (MD) algorithms
  - Produces a 128-bit hash value from an arbitrary-length message
  - Replaces MD2 and MD4
- Secure Hash Algorithm (SHA) algorithm
  - SHA-1 produces a 160-bit hash value
  - SHA-2 describes five algorithms: SHA-1 plus SHA-224, SHA-256, SHA-384, and SHA-512 which can produce hash values that are 224, 256, 384, or 512 bits in length, respectively
- Hashes are vulnerable to collision attacks (see next slide)
  - At this time, there is no obvious successor to MD5 and SHA-1 that could be put into use quickly

Hash Collision Attack

- In hashing, a collision attack is when a bad guy figures out a message (data of some type) that <gasp!> has the same hash value as the data you're trying to protect
  - Yes, a lot of math is involved!
- A "chosen prefix collision attack" is basically a normal collision attack on steroids
  - It's used to figure out entire documents, like digital certificates



VPN Protocols

- VPNs can use multiple protocols
  - IPSec tunnels are one way
  - SFTP (secure file transfer protocol) is another
    - SFTP is really FTP over SSH (secure shell)

Why Use Public Algorithms?

- Once upon a time…
  - The motion picture industry wanted to encrypt their movie DVDs to prevent pirating
  - They spent years developing an encryption standard and released it for use on DVDs
  - Canman and SoupaFr0g decoded the encryption program and released a program to decrypt DVDs, store, and play them

Thanks!

Questions?
Contact ispo@phoenix.gov