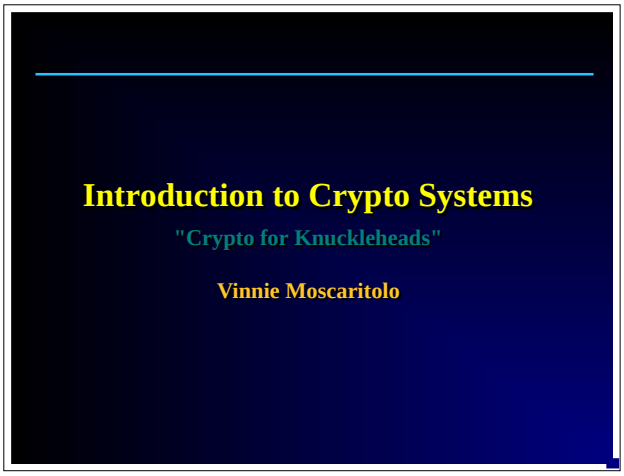
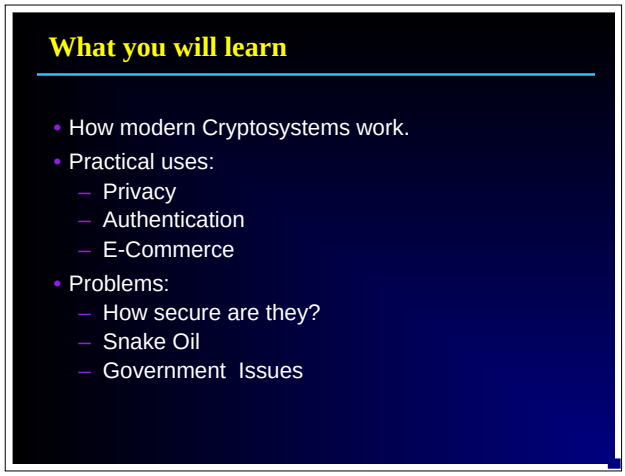
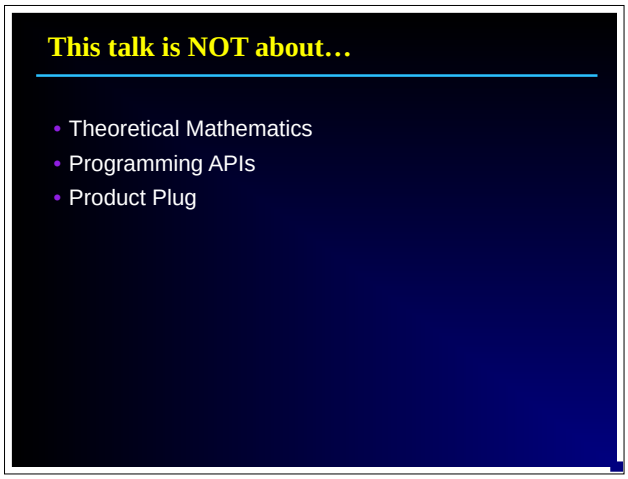


Introduction to Crypto Systems



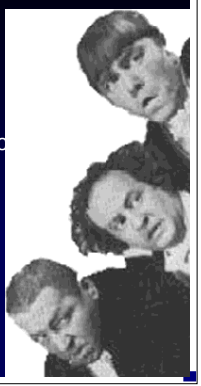
What you will learn



This talk is NOT about…

Who this talk is for

- Executive
- Marketing
- Engineer
- Anyone who needs to be Crypto co
- You?



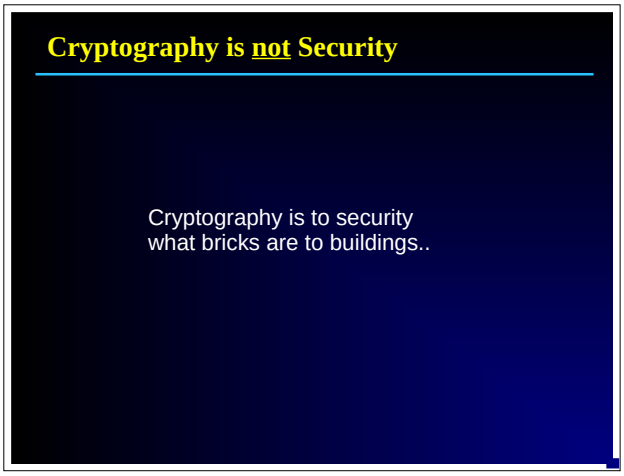
Background

- Who is Vinnie Moscaritolo ?
  - Not a Cryptographer
  - Not even a Lawyer
  - Engineer > 15 years
  - Hosts the Mac-Crypto Workshop
  - Certified Knucklehead..

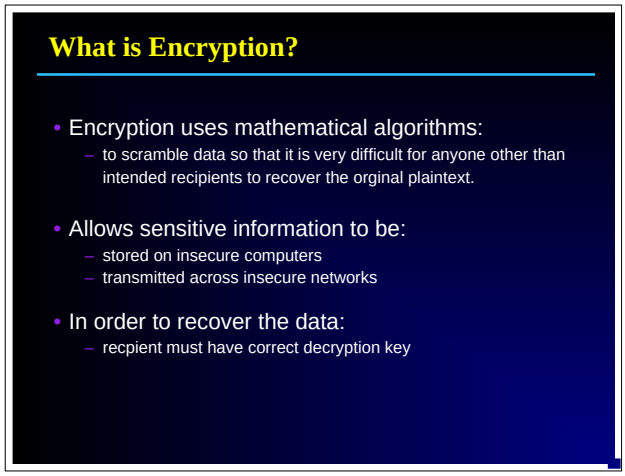
What is Cryptography?

cryp•tog•r•aphy (kríp-tog'-re-fe) *n.* The art and science of keeping messages private.

Cryptography is not Security



What is Encryption?



Cryptography is not new

Why is Cryptography important?

- People are really starting to depend on the Internet.
  - but is not a secure channel
  - In fact it's quite hostile
- Cryptography provides Privacy / Protection
  - fom competitors, business rivals, news media
  - from "Governments" (foriegn & domestic)
  - from "the Bad Guys"
- Cryptography helps keep things secret!

Why is Cryptography important?

What kind of secrets?

- Personal and Business Comunications
  - Telephone conversations, Fax , E-mail
- Financial
  - Electronic Funds Transfer
- Sensitive Biz Info
  - Trade secrets, source code, payoffs
- Critical Infrastructure Comm
  - Air Traffic Control, Power Grid, Telephone Network
- Personal Info
  - Health records, Personel files, etc

What kind of secrets?

Cryptography is not just about secrets

- Cryptography is also about trust and reputation.
  - Authentication
  - Integrity
  - Nonrepudiation

Cryptography is not just about secrets

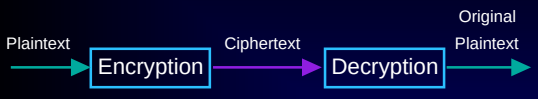
Crypto is becoming ubiquitous

- Crypto is not just for internet e-mail
- You will find it in:
  - Cellular phones
  - Cable/Sat TV broadcasts
  - radio modems
  - Smart cards
  - DVD
  - Garage door openers

How does Cryptography work?

How does Cryptography Work?

processes message with an algorithm or cipher



If no key is involved,
then the algorithm must be kept secret.
(Security through Obscurity)

Crypto is becoming ubiquitous

How does Cryptography work?

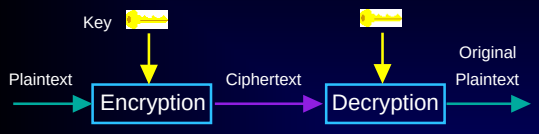
How does Cryptography Work?

Encryption without a Key

- Problems with secret algorithms:
  - Keeping it a Secret
  - Requires distribution via secure channel
  - Easy to reverse engineer
  - Lack of peer review

Encryption with a Key

- Algorithim is published.
- Key must be kept secret.



- When same key is used to encrypt & decrypt it's called a Symmetric or Secret Key Algorithm
- The secret key used for a comm session or message is called the Session Key

Key vs. Passphrase

- Key
  - Must be random
  - All keys must be equally probable
- Passphrase
  - Must be easy to remember
  - Actually has smaller keyspace
  - Dictionary attack

Secret Key Encryption Algorithms

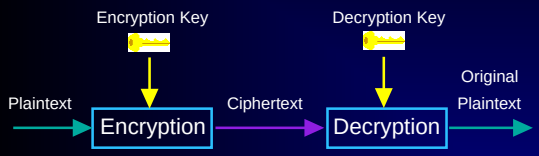
- DES - 56 bit key (easily broken with special hardware)
- 3 DES (more secure)
- IDEA - 128 bit key
- RC2/RC4 - key size variable
- BlowFish - key size variable
- CAST - Northern Telecom, 128 bit key
- SkipJack - 80 bit Key (used in clipper)

The problems with Secret Keys are..

- Selecting a Secret Key that can't be guessed
  - Is the algorithm predictable?
- Negotiating the shared secret key across an unsecured channel and still keeping it a secret.
  - Key Distribution
  - Key Security

Public Key Encryption

- Different key for encrypt and decrypt operations
- Invented in 1976
  by Whitfiled Diffie and Martin Hellman



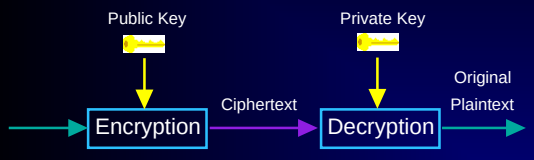
Secret Key Encryption Algorithms

The problems with Secret Keys are..

Public Key Encryption

Public Key Encryption

- Key Pairs
- Publish one key - keep other secret.
- Anyone who wants to send you a message encypts it with your public key.
- To read the message you decrypt it with the private key.



Public Key Encryption

Public Key Encryption

- A good public key algorithm:
  - Infeasible to derive one key from other.
  - Keys are interchangable
- Simplifies (but doesn't solve) key distribution problem
- Public Key is slower than Secret Key Algorithms
  - (RSA is about 1000-5000 times slower than DES)
  - Public Key Encryption is sometimes used to encrypt a Secret Key Algorithms Session key

Public Key Encryption

Public Key Encryption Algorithms

- RSA (Rivest, Shamir, Aldeman)
  - gets security from difficulty of factoring large (100 - 200 digit) prime numbers.
  - considered secure when longer (>768 bit) keys are used
- El Gamal
  - gets security from difficulty of calculating discrete logarithms in a finite field.
  - security similar to RSA for same key lengths

Public Key Encryption Algorithms

Public Key Encryption Algorithms

- Elliptic Curve
  - Shows promise for future cryptosystems.
  - More resistant to brute force attack
  - Highest crypto strength per bit of key
    - 160 bit EC key ≈ 1024 bit RSA key ≈ 10^{12} MIPS years
    - 320 bit EC key ≈ 5120 bit RSA key ≈ 10^{36} MIPS years
  - Shorter key = Savings in storage, computation, bandwidth
- Elliptic Curve Cryptography is ideal for
  - limited computation power (Smartcards, wireless devices, etc)
  - intensive use of signing or encyrption (web based TP)
  - high speed/ bandwidth devices

Public Key Encryption Algorithms

Algorithms Patents

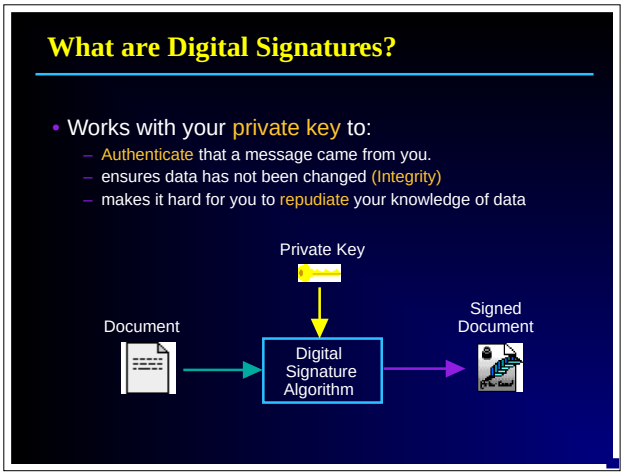
- RSA - US only, expires Sep-20-2000
- DH - patent by Cylink, expires Sept-6-1997 (GATT)
- IDEA - patent by Ascom Systec AG, Switzerland
- DES - patent by IBM, patent is expired
- RC2, RC4 were trade secrets
  - implemetation were published on net
  - names are protected by trademark
- Blowfish - not patented
- ElGamal - not patented , but Cylink claims to all public key
- Elliptic Curve - one of the patents owned by Apple

I Am Not A Lawyer!!

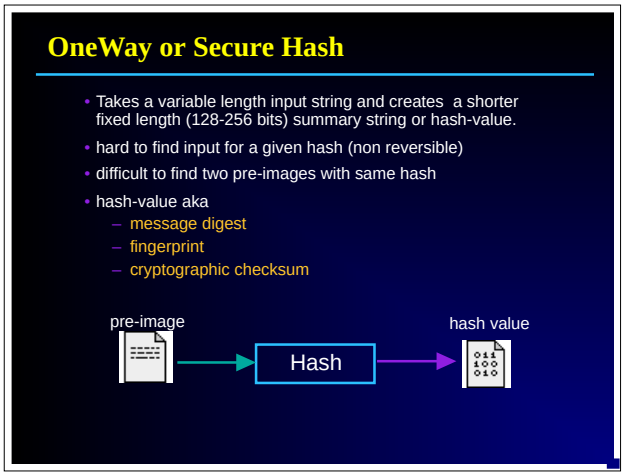
Algorithms Patents

Digital Signatures

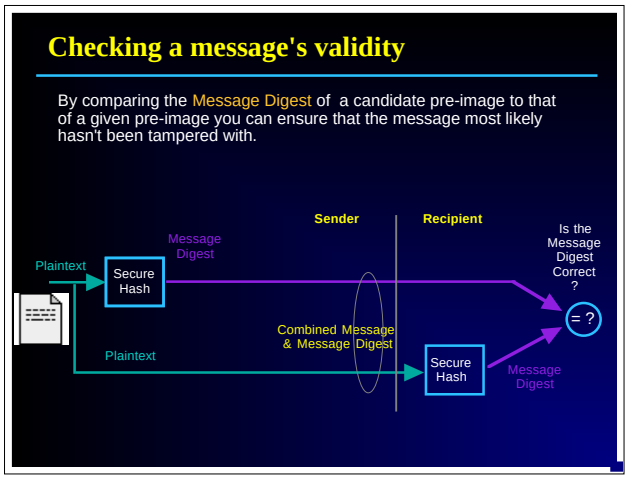
Digital Signatures



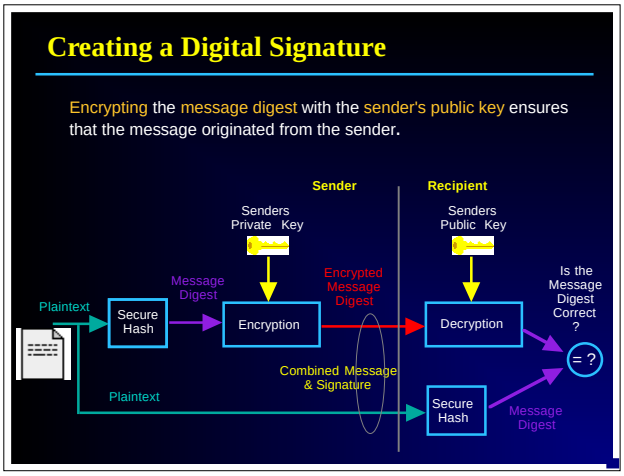
What are Digital Signatures?



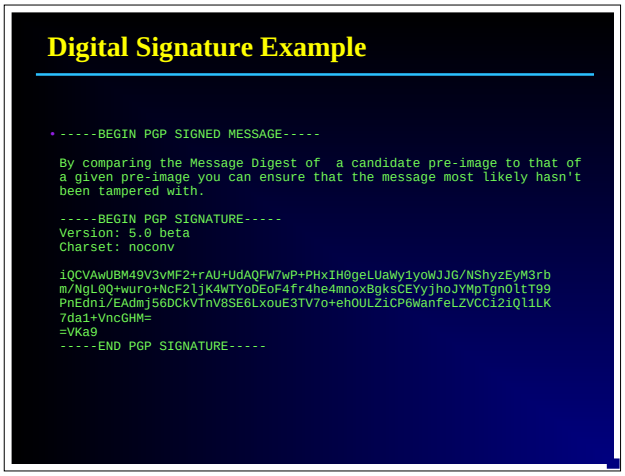
OneWay or Secure Hash



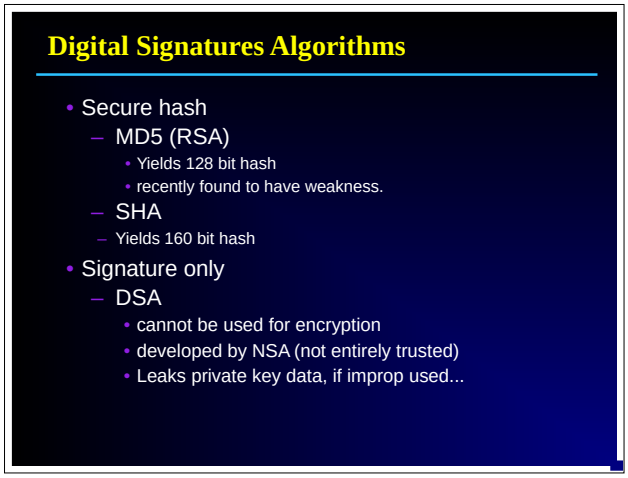
Checking a message's validity



Creating a Digital Signature



Digital Signature Example



Digital Signatures Algorithms

Digital Signature Uses

- Signatures can be used on
  - Text
  - Code (virus detection)
  - Public Keys
  - Other signatures
- Signatures can be used with
  - Timestamps
  - Name & Directory Servers
  - Software Distributions

Other Digital Signature Modes

- Standard Digital Signature requires:
  - signer to know contents of message
  - anyone with public key can verify correctness of signature without consent of signer
  - self-authenticating
- Blind Signatures
  - sign without being able to read contents
- Group Signatures

Keys and Key Management

Key Mangement

- Key management is hardest part of cryptography
- Answers the questions
  - How do I get a key pair?
  - How do I get someone else's public key?
    - and how do I know its really theirs?
  - What should I do if I lose my key?
    - or it's stolen?
  - How long is my key good for?

Key Mangement

Lifetime of a Key

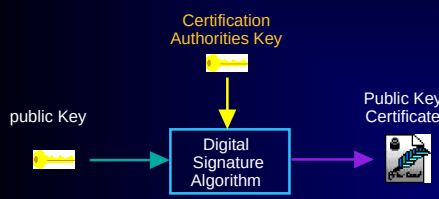
- Creation & Registration
  - centralized (Kerberos) / distibuted (RSA, PGP)
- Certification
  - centralized (X.509) / distibuted (PGP)
- Distribution
  - introduction (PGP)
  - storage / backup (escrow)
- Usage
  - validity checking
- Termination & Revokation
  - deliberate destruction or expired
  - archival

Lifetime of a Key

Certification & Trust Management

Q: How does Alice know that a public key is Bob's and not someone pretending to be Bob ?

A: Bob's public key is signed by a trusted entity.



Certification & Trust Management

What kinds of Certificate?

- Identity Certificate
  - Binds the name of an idenity to a public key.
  - X.509, PGP
- Meta Certificate
  - Delegates an attribute or authority to a public key.
  - SPKI

What kinds of Certificate?

Identity Certificates

- X.509
  - Originates from X.500 database design
  - Names are organized into a hierarchy
    - Corporate roles, Notarized Documents.
  - Requires Certificate Authority (CA)
- PGP
  - Signer of key might not be known or trusted
  - Allows independent signatures to vote a binding into validity
  - "Web of Trust"

Identity Certificates

X.509 Certificate

- Each user has distinct name
- Signed by heierachial CA
  - tree stucture
- Protocol to verify validity
- Keys can be
  - individuals
  - groups / organizations

Version
Serial number
Algorithm Identifier: - Algorithm - parameters
Issuer
Period of Validity: - Not before date - Not after date
Subject
Subjects Public Key: - Algorithm - Parameters - Public Key
Signiture

X.509 Certificate

PGP Certificate

- No CA that everyone needs to trust
  - no implicit guarantee of validity
  - no policy for establish trust
  - Web of trust
- Key can only be trusted if there is path of signatures between verifier and sig in question
- Keys can be
  - individuals
  - groups / organizations
  - network services
  - psuedonynms
  - anonymous addresses

PGP Certificate

KeyServers

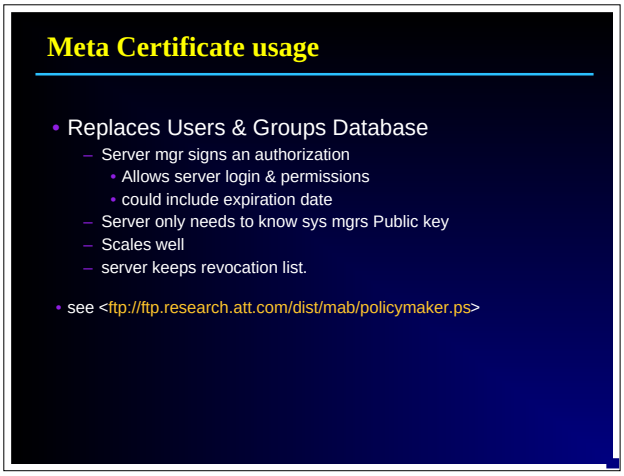
- Where do I get someone elses public key..
  - from a Keyserver
    - see <http://www.pgp.com/keyserver>
    - see <http://www-swiss.ai.mit.edu/~bal/pks-toplev.html>
- Integrated Keyserver
  - 1st Gen
    - like cache / keychain
  - 2nd Gen
    - like a directory server

KeyServers

Meta Certificates

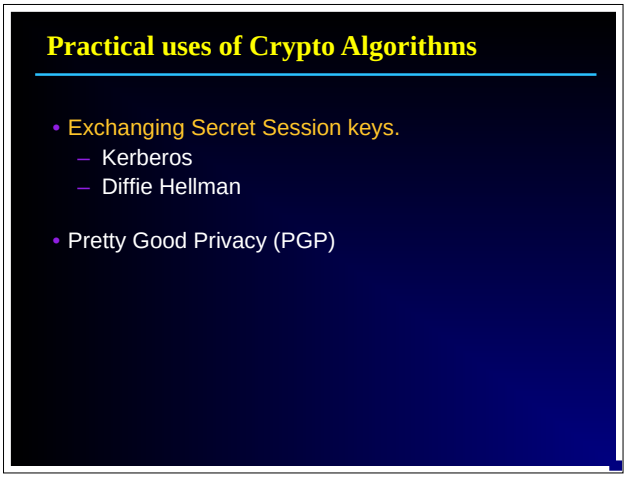
- Decentralized Trust Management
- Digitally signed, structured message which delegates an attribute (trust or authority) of some form to a public key
- Simple Public Key Infrastructure SPKI
  - see <http://www.clark.net/pub/cme/spki-reqts.html>

Meta Certificates



Meta Certificate usage

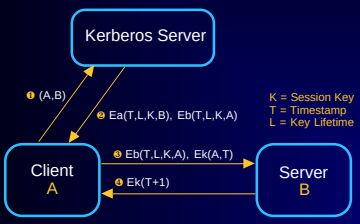
Modern Crypto Systems



Practical uses of Crypto Algorithms

Kerberos Key Exchange

- Used to agree on a shared secret sesion key , but... requires trusted third party.
- To prevent replay attack
  - Key exchange includes timestamp and lifetime of key
  - Requires clocks to be synced



Kerberos Key Exchange

❶Alice asks Sam for a key to talk to Bob

A->S: (A,B)

❷ Sam replies with sesion key K, Timestamp T, and its Lifetime L. encypted with Alice's and Bob's key,

S->A: Ea(T,L,K,B), Eb(T,L,K,A)

❸ Alice relays the encrypted session key to Bob

A->B: Eb(T,L,K,A), Ek(A,T)

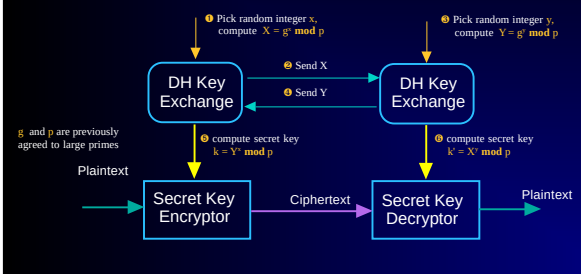
❹ Bob shows Alice that it knows the key by using it.

B->A: Ek(T+1)

Kerberos Key Exchange

Diffie-Hellman Key Exchange

- Used to agree on a shared secret sesion key w/o third party
- Assumes communication channel is not secure
- Reveals nothing useful to wiretapper



Diffie-Hellman Key Exchange

Diffie-Hellman Key Exchange

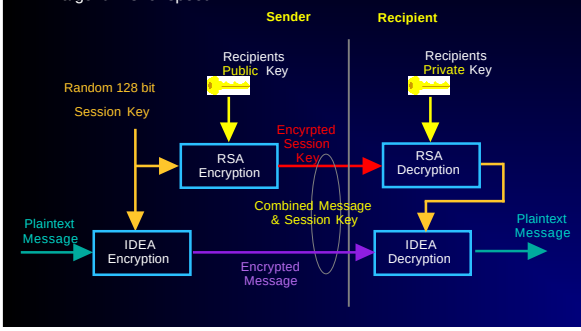
1. Alice and Bob agree to a large prime, p and a generator g
2. Alice generates a random, secret quantity, x
3. Bob generates a random, secret quantity , y
4. Alice computes $X = g^x \bmod p$
5. Bob computes $Y = g^y \bmod p$
6. A->B: X
7. B->A: Y
8. Alice computes $k = Y^x \bmod p$
9. Bob computes $k' = X^y \bmod p$
10. Alice and Bob use the secret key $k = k'$ to encrypt their session

Diffie-Hellman Key Exchange (Notes)

- To defeat Man in Middle Attack
  - Transmit the resulting k (or secure hash) to each other.
  - PGPfone does this with a Biometric signature
- Destroy Keys after session is terminated:
  - Back Traffic Protection (BTP)
    - compromising the keys for one session doesn't reduce security of past sessions
  - Perfect Forward Secrecy (PFS)
    - compromising the keys for one session doesn't reduce security of future sessions

Pretty Good Privacy (PGP)

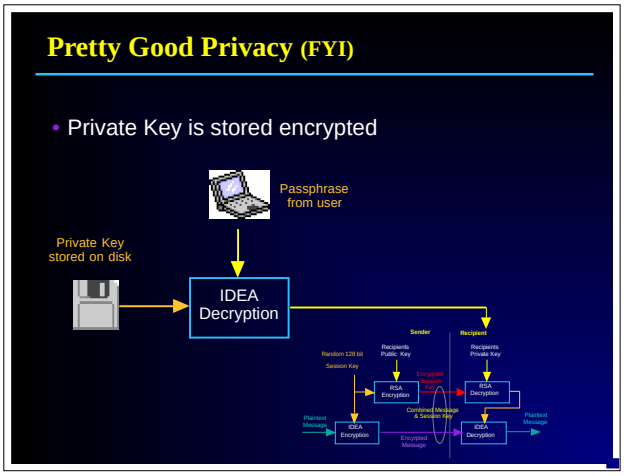
Combines use of RSA (public key) and IDEA (Symmetric key) algorithms for speed.



Diffie-Hellman Key Exchange

Diffie-Hellman Key Exchange (Notes)

Pretty Good Privacy (PGP)



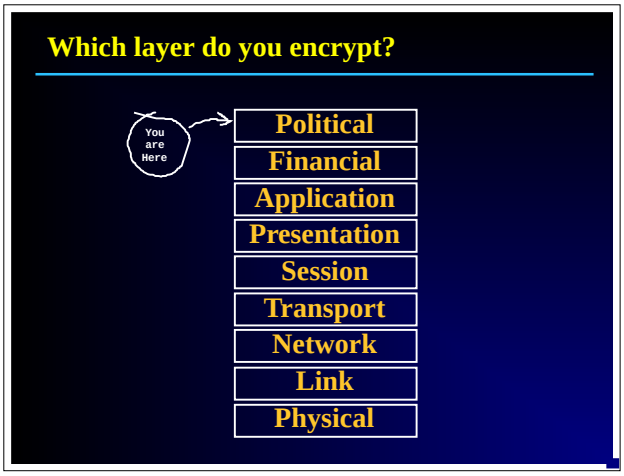
Pretty Good Privacy (FYI)

Crypto on the Internet

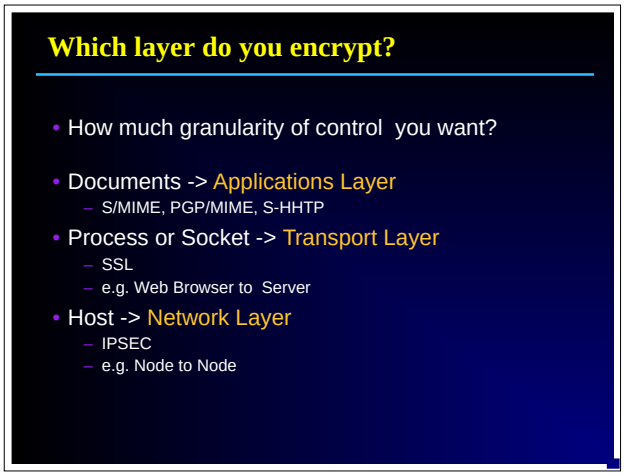
Internet threat model

- The internet is an insecure channel
- Assume:
  - *anything* you say is overheard
  - *everything* you say is overheard
- Never send any secure info in the clear
  - "passphrases over telnet"

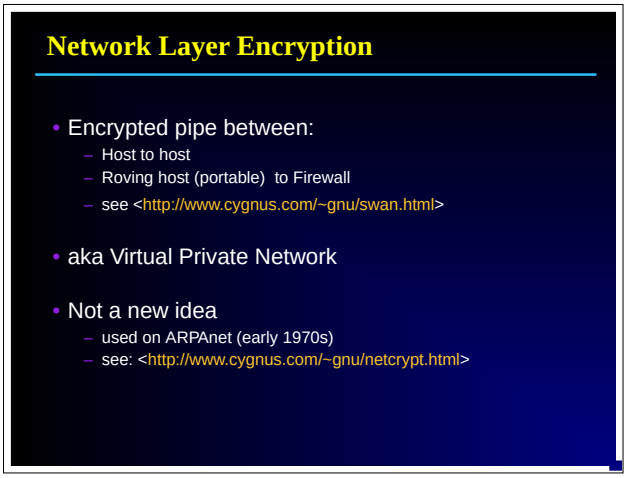
Internet threat model



Which layer do you encrypt?



Which layer do you encrypt?



Network Layer Encryption

Network Layer Encryption

- Internet Protocol Security (IPSEC)
  - Encrypted pipe between hosts or firewalls.
  - IPv6 requirement, IPv4 optional
  - see RFC 1825
- Authentication
  - Uses X.509 certs
  - Authentication Header (AH)
  - RFC 1826, RFC 1828 (MD5), RFC 1852 (SHA)
- Encryption
  - Encapsulating Security Payload (ESP)
  - RFC 1827, RFC 1829 (DES), RFC 1851 (3DES)
- AH & ESP may be use together or separate
- see <http://www.cs.arizona.edu/xkernel/www/ipsec/ipsec.html>

Network Layer Encryption

IPSEC Key Management

- Currently (6/5/97) two incompatible schemes
- Simple Key Management Protocol (SKIP)
  - Sun Microsystems
- Internet Security Association Key Management Protocol (ISAKMP / Oakley)
  - NSA

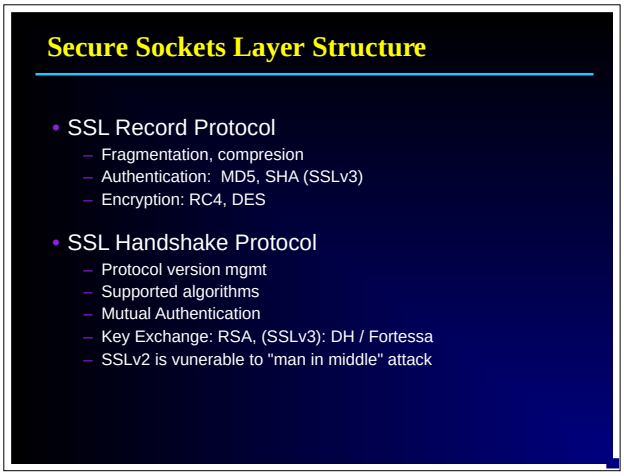
IPSEC Key Management

Transport Layer Encryption

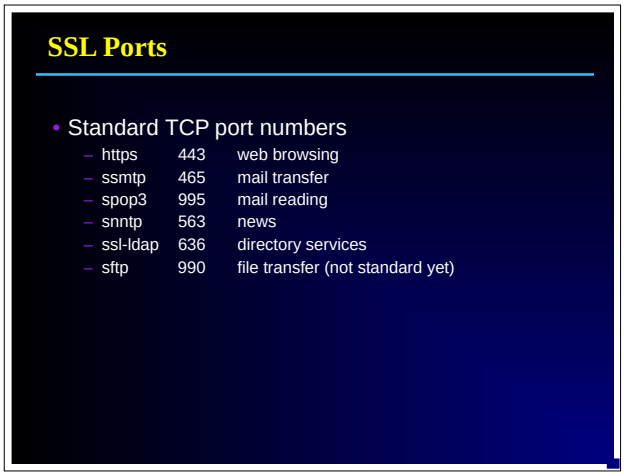
- Encrypted pipe between processes
  - Layered on top of reliable transport
  - Most network applications must be modified for support
  - Doesn't handle datagrams (UDP)
- Secure Socket Layer (SSL)
  - Netscape
- Private Communications Technology
  - Microsoft
  - based on SSLv2
- Transport Layer Security (TLS)
  - IETF working group
  - Based on SSLv3
- SSL FAQ:
  - <http://www.consensus.com/security/ssl-talk-faq.html>

Transport Layer Encryption

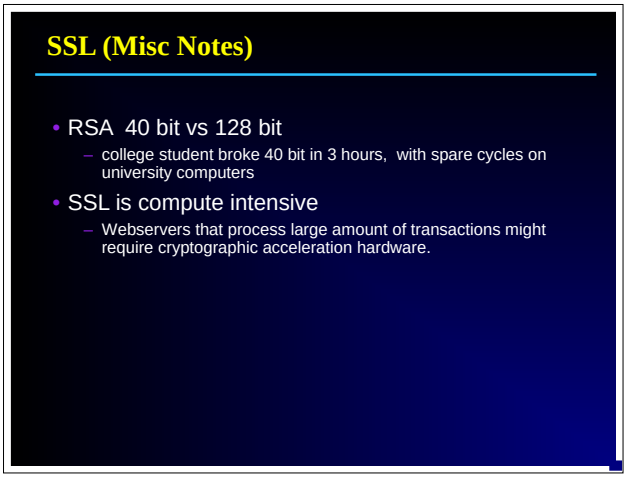
Secure Sockets Layer Structure



SSL Ports



SSL (Misc Notes)



Applications Layer Encryption

- Secure at document level
- Encrypted or Authenticated files
  - E-mail , text files, www pages

```
-----BEGIN PGP SIGNED MESSAGE-----

this is a signed message by vinnie

-----BEGIN PGP SIGNATURE-----
Version: 5.0 beta
Charset: noconv

iQCVAwUBAAAAAPMF2+rAU+UdAQGJVwP/bECEW3QnMdtZl7jNwJxNOcae5tqQKo1i
7sH2ifzu3yfhwGenQDOg0dtb5yWbMqTomZRyRjMwl3LvlNI53T6xdTUa1M23zBCr
r6FGewxDvp9EXNcJgRg10X2dZRqU0jG5bESCbCEoqIIyBRD/u1KAEap5LPa8wKB2
3hBz7vYEk9g=
=eSwI
-----END PGP SIGNATURE-----
```

Crypto in Email

- E-mail
  - PEM (RFC 1421-24)
    - Failed because lack of PKI
  - S/MIME, PGP/MIME
    - In use today!

Anonymous Remailers

- Provides mail w/o receiver knowing your name or e-mail address
- Allows user to speak w/o fear of reprisal
  - Apple "Can We Talk"
  - alt.child.abuse.recovery, etc
- Original remailer
  - A script that allowed anonymous posts into <alt.sex.bondage> !
- Cypherpunk remailer
  - attacked by monitoring length of packets
- MixMaster
  - Uses fixed length packets
  - see <http://www.stack.nl/~galactus/remailers/>

Crypto on the WWW

- S-HTTP
  - Enterprise Integration Technologies / Terisa
  - extension to http
  - documents can be marked as private or signed
  - supports most crypto algorithms
  - NOT A STANDARD!!
- See: <http://www.eit.com/creations/presentations/shttp-ams/>
- See: <http://www.terisa.com>

Crypto on the WWW

Electronic Commerce

"Digital Commerce is Financial Cryptography"
- Robert Hettinga, 1994

Electronic Commerce

E-Commerce is Finacial Cryptography

- Electronic commerce depends on cryptography
  - to make binding commitments
- IDC estimates e-commerce market will be worth > $200B by 2000
  - But only if systems are very secure

$$$$$

E-Commerce is Finacial Cryptography

Kinds of E-Commerce

- Book Entries
  - uses encrypted channel to pass debit & credit info
  - requires double entry book keeping via intermediary
- Electronic Cash
  - Cryptographic objects that have monetary value assigned to it.
  - Bearer Certificates
  - Peer to Peer transaction.
  - requires mint or underwriter to issue coins

Kinds of E-Commerce

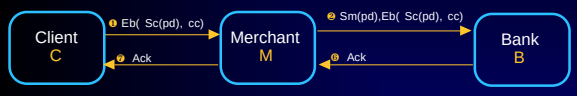
Book Entry Systems

- Cybercash
  - Encrypted credit cards ... BFD
- First Virtual
  - Requires account, not encypted, wants to be a bank...
- Mondex
  - Bank puts book entries on smartcard, good for small amounts
- SET
  - Credit card numbers exchanged
- Electronic Checks
  - Financial Service Technology Consortium

Book Entry Systems

Secure Electronic Transactions (SET)

- Intent was merchant can't see credit card #
  - but now has back channel for non-repudiation
- Process is slow



pd = Product description
cc = Credit card number

❸ Decrypt Eb(Sc(pd), cc)
❹ Compare Sc(pd) = Sm(pd)
❺ proccess cc - pd

Secure Electronic Transactions (SET)

Bearer Certificate Systems

- Milicent
  - Site issues values that can only be spent there.
- Digicash
  - Anonymous Digital Cash!!
- Bearer Bonds
  - Application of Digicash Patent

DigiCash

- Cryptographic objects that have monetary value assigned to it.
- Anonymous Digital Cash
- Chaum patent expires in 2007
  - bank->sw mfg->cc assos
  - by the time they figure out biz model, patent will expire
  - Dolby model

DigiCash's E-cash Protocol

Withdraw Coins

1. Client generates a 20 byte random coin serial number.
2. Client blinds the serial number with random blinding factor.
3. Client sends blinded serial number and coin denomination wanted to mint.
4. Mint signs blinded serial number with denomination dependent secret key.
5. Client unblinds coin serial number, mint signature is still valid.
6. Client sends coin to shop.

Deposit Coins

1. Shop sends coin to mint.
2. Mint checks it's database to see if coin has already been spent.
3. If coin hasn't been spent, the mint credits the shop's account.

Smart Cards

- Limited processing power & memory
  - Java Wallet
- provides offline secure storage
  - digital cash
  - private keys
  - etc
- Will quickly become the most prolific peripheral...

Smart Cards

How Secure are Crypto Systems?

How Secure are Crypto Systems?

Security of Algorithms

- Cryptanalysis
  - The art and science recovering the plaintext of a encrypted message without access to the key.
- Strong vs Weak Crypto
  - An algorithm is computationally secure or strong if it cannot be broken with available resources (both present and future)?
- Rule of Thumb
  - The value of data must remain less than the cost of breaking the security protecting it.

Security of Algorithms

Who can break a crypto system?

- Government Intel agency
  - NSA
- Large Corporations
- Organized Crime
- College students
  - with spare time from a bunch of computers

Cost of breaking Crypto (brute force)

Type of Attacker	Budget	Tool	Time and Cost per key recovered 40 bits	56 bits	Length Needed for for protection (late 1995)
Pedestrian Hacker	tiny	scavenged computer time	1 week	infeasible	45
	$400	FPGA	5 hrs ($0.08)	38 yrs ($5,000)	50
Small Business	$10,000	FPGA	12 min ($0.08)	556 days ($5,000)	55
Corporate Department	$300K	FPGA	24 sec ($0.08)	19 days ($5,000)	60
		ASIC	.18 seconds ($0.001)	3 hours ($38)	
Large Corporation	$10M	FPGA	.7 sec ($0.08)	13 hrs ($5,000)	70
		ASIC	.005 sec ($0.001)	6 min ($38)	
Intellegence Agency	$300M	ASIC	.0002 sec ($0.001)	12 sec ($38)	75

Strength of crypto depends on key quality

- Keyspace
  - Size and distribution
  - Key Generation Algorithm
    - how random is random?
    - see <http://www.merrymeent.com/jon/usingrandom.html >

Keyspace		4 Byte	8 Byte
Lowercase Letters	(26)	460,000	$2.1*10^{11}$
Lowercase Letters & digits	(36)	1,700,000	$2.8*10^{12}$
Alphanumeric characters	(62)	$1.5*10^{7}$	$2.2*10^{14}$
Printable characters	(95)	$8.1*10^{7}$	$6.6*10^{15}$
ASCII characters	(128)	$2.7*10^{8}$	$7.2*10^{16}$
8 bit ASCII characters	(256)	$4.3*10^{9}$	$1.8*10^{19}$

Who can break a crypto system?

Cost of breaking Crypto (brute force)

Strength of crypto depends on key quality

Sometimes size isn't everything.

Method :

Secret	vs	Public
56 bit DES	≈	512 bit RSA
340 Bit RC4	≈	320 bit RSA

Algorithm:

160 bit EC	≈	1024 bit RSA
320 bit EC	≈	5120 bit RSA

Internet DES Cracking effort

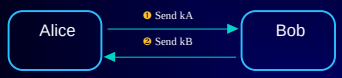
- DESCHALL
  - see <http://www.frii.com/~rcv/deschall.htm>
- Broke 56 Bit DES
  - via brute force keysearch
- Distributed computing on internet
  - Aprox 14,000 machines
  - Spare CPU time (screen saver)
  - Searched 25% of keyspace in 5 Months (32 days if full time)
  - Peak speed: 7 B keys / sec, 500 Mips years
  - Cost < 10K

Cryptographic Attacks

- Passive attacks
  - Cyphertext only attacks
  - Known plaintext attacks
  - Traffic Analysis
- Active attacks
  - Chosen plaintext
  - Man in the middle
  - Rubber hose
- Bypass the Cryptosystem...
  - plant a bug in the room
  - Tempest attack

Example of Man in the Middle Attack

Bob and Alice want to exchange public keys
They assume the communication channel is secure



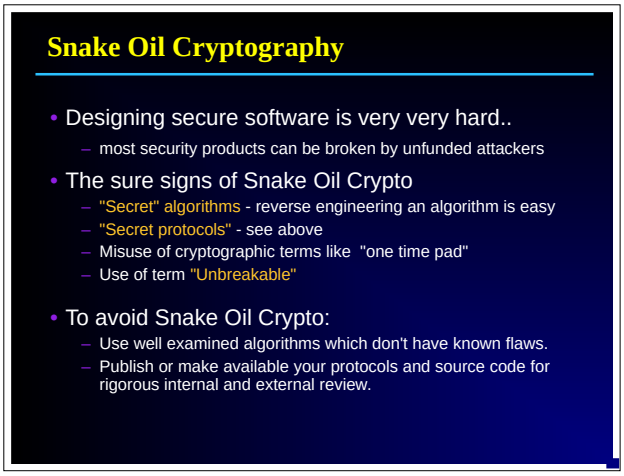
Example of Man in the Middle Attack

Eve has intercepted the comm channel
and acts as an imposter to Bob and Alice
Alice and Bob think that they have each others keys
But actually have Eve's version of the keys

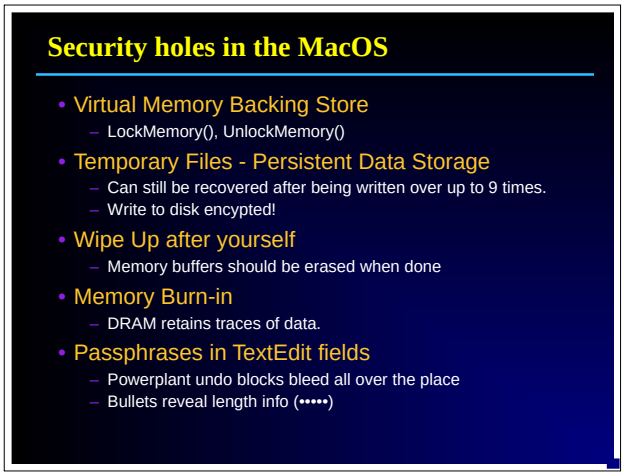
Result: Eve can read and even modify all comm between Bob and Alice, and they are unware of any interference.

One Time Pad

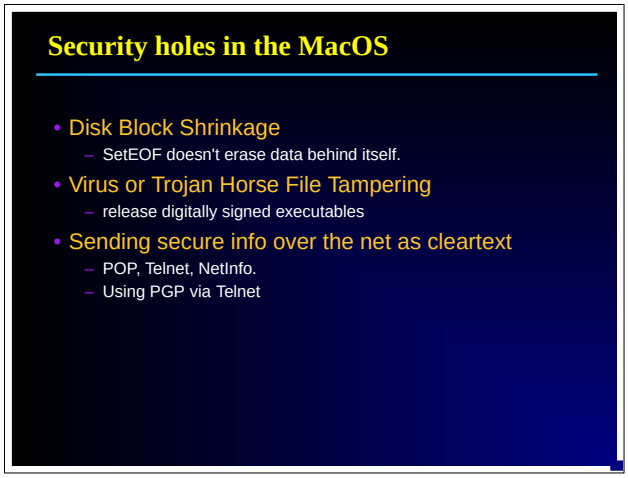
- Used to generate Secret Key
  - Key is only once for one message
  - Key is destroyed after use
  - Should not be generated by algorithm
  - requires specialized hardware that collects randomness
- Used in ultra-secure, low bandwidth channels
  - Hotline from Washington D.C. to Moscow
  - Distributed by courier



Snake Oil Cryptography



Security holes in the MacOS



Security holes in the MacOS

Crypto and the Government

Crypto and the Government

History Lesson

History Lesson

- In 1993, NSA figured out that they couldn't stop progress
  - Strong crypto would soon be ubiquitous
- Informed FBI, phone taps would no longer work
  - Louis Freeh made his rep by bugging mobsters
- FBI freaked!
  - "Uncrackable encryption will allow drug lords, terrorists, and even gangs to communicate with impunity, ... and will devastate our ability to fight crime and prevent terrorism. "

    -- Louis Freeh

US Government response

US Government response

- Export restrictions on strong Cryptography
- Government want access to private keys

Export Restrictions on Strong Crypto

Strong crypto is viewed as threat to national security
- Unlawful to export (import is OK, for now)
- Classified as munition!
- International Traffic in Arm Restrictions (ITAR)

Reality:
- strong crypto is very available worldwide

Results:
- Weakens US corp defenses against foriegn intel
- Forces US products to be less competetive
- Lost jobs for US (est. $60B by year 2000)

Government want access to private keys

- Agencies seeking to conduct covert surveillence
  - claim the wide availability of strong crypto technology is a serious threat to law enforcement, public safety and national security.
  - fear that crypto will be used by organized crime,terrorists money launders and child pornographers.
  - want to guaranteed access to encrypted information without the knowledge or consent of owner.
  - insist that it won't be abused or comprimised.
  - claim that it can be done safely.

It's really about money (no surprise)

- Encryption on internet & e-commerce.
- Internet based biz move to offshore tax havens
  - Anguilla, FC97
- If flow of money among citizens becomes invisible
  - currency regulations become unenforceable
  - taxes become uncollectable.
- see <http://www.arraydev.com/commerce/JIBC>
- see <http://www.shipwright.com>

Export Restrictions on Strong Crypto

Government want access to private keys

It's really about money (no surprise)

GAK by any other name

- Government Access to Keys (GAK)
  - aka Key Escrow, Key Recovery, Data Recovery
- For GAK to work, you need:
  - That non-escrowed cryptosystems uninvent themselves.
  - A method external to the cryptosystem to decode encrypted data.
  - A way to transport and store a highly sensitive secret key for an extended period of time.
  - A large scale key management system
  - LEA requires high availability (24-7), access to keys within 2 hours, under current regulations.

GAK by any other name

Storage recovery vs Comm recovery

- Storage recovery
  - legitimate need
  - secret sharing tech
  - local key registry
  - encryption of session key to multiple recipients
- Communication recovery
  - No commercial incentive to develop this technology
  - Only useful for wire tapping
  - If a session key is lost data can be re-transmitt
  - Requires a copy of session key be securely retained until sent to escrow agent.
  - (Every cell phone, FAX, secure web session be escrowed)

Storage recovery vs Comm recovery

What about...

- Risks
  - Improper disclosure of keys
  - Theft of keys
- Complexity
  - Strong crypto is hard to design
  - Scale (are you going to store every session key?)
  - Operational complexity
- Costs
  - Operational
  - Product
  - Government Oversight
  - User Costs
- see <http://www.crypto.com/key_study>

What about...

Oh and that pesky document..

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated..

AMENDMENT IV, The Bill of Rights.
Passed by Congres September 25, 1789

Summary

Summary

We are almost at the end..

What have we learned

What have we learned

- Cryptography is more than secrets
- It's also be about Trust and Reputation.
- Required for E-Commerce
- Good Cryptography is hard to do
  - Avoid Snake Oil Crypto
- But shouldn't be hard to use.

For more info.

Applied Cryptography, Second Edition, Bruce Schneier
Great review of current protocols and algorithms

The Code-Breakers, David Kahn
History of cryptography

Internet Crypto resources
<http://www.vmeng.com/vinnie/crypto.html>

For more info.

Q&A

Q&A

Cryptography

the power to…

mQCNAirJ6tMAAAED/jj6Y2npP4R2LbUC9CxJ4KugRXYriztbryfVjp/SmfifqZ4/
204wyWVCaWEiVjW/wJKHZD/PtetocFK8BHyo7fancvYkp6Gx2x1RjDhuv+sgAhtO
1BWh3HB51FWHBVojVg6g4AStHU3mhDb4EvdF2EfNnJPz9nUi/71LYmqiC9QjAAUR
tDdaYmlnbmlldyBGaWVkb3Jvd2ljeiA8ZmllZG9yb3dAbWF0aC5tcHMub2hpby1z
dGF0ZS5lZHU+iQCVAgUQLxRlhvX0zg8FAL9FAQGXJgQA1ZITkWIj7SEt++AZa7wj
Jlx+wTqox2bZ7oox/i2FQSZLBvd15z08eHVgF4GuALS051hY05c9tNV4XSJ9ZAFA
v/z4UUrImEit6PMlEIQDffNylYhreYg97X2HNj4WiLty6ecuHEGWigkzGUz3+9cT
nNA7F+2eIzY/eJHtVAKIcJSJAJUDBRAsdOBFvUtiaqiL1CMBAwQoA/kBjsuoeuix
+rJ+igY0eCshSBz9sTs9o4FkWVYoiBWe4nWjkvQGO65FTJinm5qpBVWGLVe7fiUh
/ox+QrEdFNFvNyFqUIVyMjES43zOH6eePcuBiY8XJwppWoFw45TLfXe9XLvrE6ol
N2P3vM2RG5g/xeKHK5lS9lPERxFnOtCU67QuWmJpZ25pZXcgRmllZG9yb3dpY3og
PHppZ2ZAbXBzLm9oaW8tc3RhdGUuZWR1PokAlQIFEC73bob19M4PBQC/RQEBBegD
+wUdgN5sDnrtKpClokWUpYcuR74SZUTj3VSlD7ipfw5CJpGILAVijoe0o8PA+k1A
69et98C5uR9yKVqHyxFUnl1ZlomFeyUjx1laTAYOF7pjnXrlvEVa6HBaTeMKyBvc

Q&A