Cryptography

Stephen White

19 February 2004

Introduction

We need to pass a private message over an insecure medium.

- Internet
- Telephone/Telegraph
- Radio Transmissions
- Even letters can be intercepted

Introduction

We need to pass a private message over an insecure medium.

- Internet
- Telephone/Telegraph
- Radio Transmissions
- Even letters can be intercepted

We could hide the message, “steganography”.

- If the message is discovered (deliberately or accidently) then it's meaning is quickly discovered.
- Relies of knowing ways of hiding the message that an *attacker* doesn't.

Introduction - steganography

There are many forms, which have been used for over 2500 years.

- Writing a message on a wax tablet, but below the wax
- Microdots were used during WWII
  - a full stop in a message contains the hidden message
- The Victorians put pin-pricks below letters on a newspaper page to spell out the message

Introduction

The alternative is to scramble (encrypt) the message in order to prevent it being read. We need to make sure that it's:

- Easy to decrypt by people that we want to read the message
- Hard to decrypt by people that we don't want to read it

Introduction

The alternative is to scramble (encrypt) the message in order to prevent it being read. We need to make sure that it's:

- Easy to decrypt by people that we want to read the message
- Hard to decrypt by people that we don't want to read it

We could re-order parts of the message (“transposition”), for example the Spartan Scytale. The message is written on a belt wrapped around a piece of wood. The message can only be easily read by wrapping the parchment around another piece of wood of the same dimensions. Much information from the original message remains intact (for example, it contains the same letters) so such ciphers are generally fairly easy to crack.

Substitution ciphers

- Replace each letter in the alphabet with another.
- Simplest form is a 'Caesar Cipher'

Substitution ciphers

- Replace each letter in the alphabet with another.
- Simplest form is a 'Caesar Cipher' – poor keyspace

Substitution ciphers

- Replace each letter in the alphabet with another.
- Simplest form is a 'Caesar Cipher' – poor keyspace

Can be made more complex:

- Arbitary mappings between letters (not just shifts)

Substitution ciphers

- Replace each letter in the alphabet with another.
- Simplest form is a 'Caesar Cipher' – poor keyspace

Can be made more complex:

- Arbitary mappings between letters (not just shifts)
  - used lots during the first millenium, but vulnerable to frequency analysis (as discovered by the Arabs)

Substitution ciphers

- Replace each letter in the alphabet with another.
- Simplest form is a 'Caesar Cipher' – poor keyspace

Can be made more complex:

- Arbitary mappings between letters (not just shifts)
  - used lots during the first millenium, but vulnerable to frequency analysis (as discovered by the Arabs)
- Add nulls or alternative mappings for common letters

Substitution ciphers

- Replace each letter in the alphabet with another.
- Simplest form is a 'Caesar Cipher' – poor keyspace

Can be made more complex:

- Arbitary mappings between letters (not just shifts)
  - used lots during the first millenium, but vulnerable to frequency analysis (as discovered by the Arabs)
- Add nulls or alternative mappings for common letters
  - "Friendlyness" of letters can help identify mappings
  - also use frequency analysis (including consideration of common words)

Substitution ciphers

- Replace each letter in the alphabet with another.
- Simplest form is a 'Caesar Cipher' – poor keyspace

Can be made more complex:

- Arbitary mappings between letters (not just shifts)
  - used lots during the first millenium, but vulnerable to frequency analysis (as discovered by the Arabs)
- Add nulls or alternative mappings for common letters
  - “Friendlyness” of letters can help identify mappings
  - also use frequency analysis (including consideration of common words)

All varations, including encrypting syllables rather than letters and nomenclators, can be broken using these methods.

Polyalphabetic substitution ciphers

- Use different mappings (alphabets) when encrypting different letters from the message
- Examples include the Vigenère cipher, where a codeword is used to select how to encrypt each letter

Polyalphabetic substitution ciphers

- Use different mappings (alphabets) when encrypting different letters from the message
- Examples include the Vigenère cipher, where a codeword is used to select how to encrypt each letter

The Vigenère cipher was broken in the mid 1800s by Babbage, who didn't publish his work, and broken again shortly afterwards by Friedrich Wilhelm Kasisk.

- Find patterns that occur multiple times in the ciphertext
- Deduce length of codeword from the divisors of the distances between them
- The polyalphabetic cipher can then be considered as a set of monoalphabetic ciphers and cracked

One-time pad

- A polyalphabetic cipher with a codeword (key) longer than the message
- Truly unbreakable
- Developed by the US in 1918

One-time pad

- A polyalphabetic cipher with a codeword (key) longer than the message
- Truly unbreakable
- Developed by the US in 1918

Problems:

- Key must be totally random
- Key must NEVER be used twice
- Production of enough random data
  - how much is enough going to be?
- Need to distribute huge amounts of data (the key) securely
- Encryption and decryption by hand is slow and error-prone

Mechanical and electronic devices

- Allow polyalphabetic ciphers where the same cipher alphabets are not repeated, but are calculated based on previous parts of the message
- Fast and error free
- Enigma (story in itself)
- Modern computers ...

Mechanical and electronic devices

- Allow polyalphabetic ciphers where the same cipher alphabets are not repeated, but are calculated based on previous parts of the message
- Fast and error free
- Enigma (story in itself)
- Modern computers ...

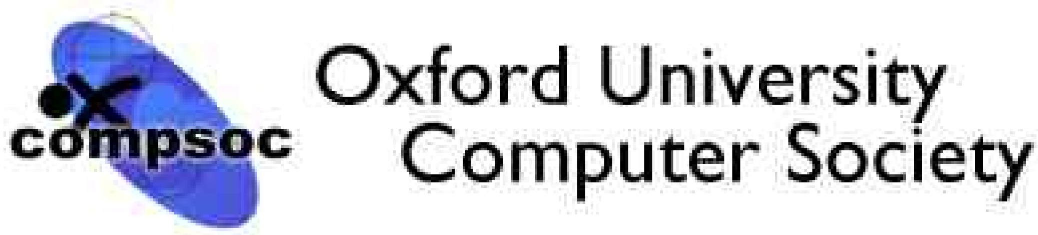
All of these are symmetric ciphers, encryption and decryption are reversals of exactly the same process.

Symmetric ciphers today

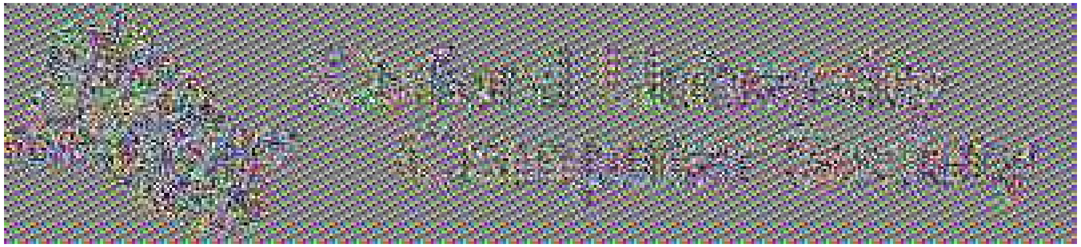
- DES, 3DES, IDEA, AES
- Generally “block ciphers” - they can encrypt and decrypt blocks of data

Symmetric ciphers today

- DES, 3DES, IDEA, AES
- Generally “block ciphers” - they can encrypt and decrypt blocks of data
- When encrypting a stream of data we must not encrypt identical blocks of data in the same way

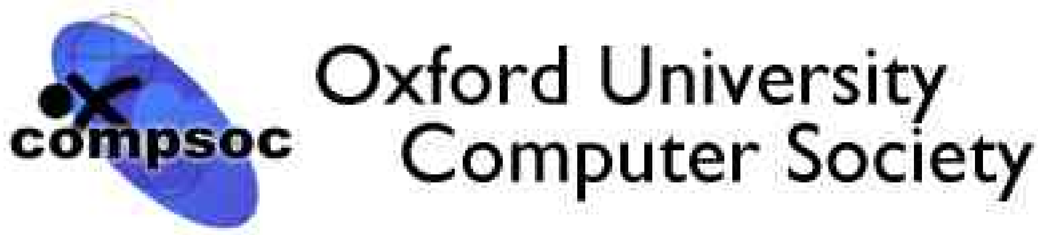


would become

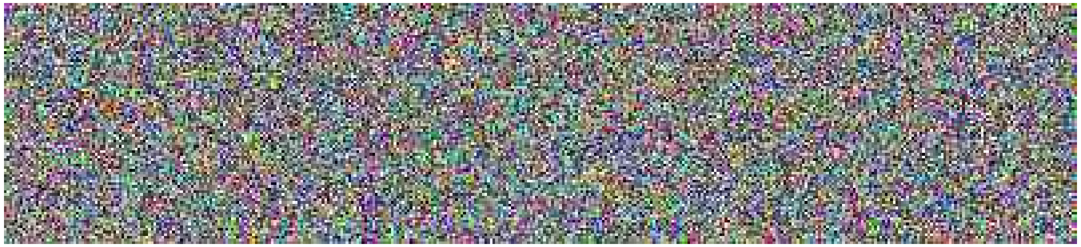


Symmetric ciphers today

- DES, 3DES, IDEA, AES
- Generally “block ciphers” - they can encrypt and decrypt blocks of data
- When encrypting a stream of data we must not encrypt identical blocks of data in the same way



combing the encrypted version of previous block with the plaintext of the current block before encrypting gives



Why doesn't the talk end here?

- It would be nice to be able to communicate securely without having to meet to agree an encryption key
- We should be able to tell if an attacker has modified the message during transmission

The first of these requirements imposes an interesting problems of it's own

- How can we securely identify the person we are communicated with if we haven't met them
- How can we be sure we aren't communicating with someone masquarding as the person we want to communicate with (the attacker may also be masquarding as us to the person we want to talk to, thus affecting a “man in the middle” attack)

Diffie-Hellman key exchange

- Allows two people to agree on a secret key over an insecure communication medium
- It is based on the fact that $G^{XY} = G^{YX}$
- It is very difficult to calculate N from G^{N} (mod P) if large numbers are used

Diffie-Hellman key exchange

- Allows two people to agree on a secret key over an insecure communication medium
- It is based on the fact that $G^{XY} = G^{YX}$
- It is very difficult to calculate N from G^N (mod P) if large numbers are used

- Alice and Bob choose two large numbers, a prime P and an integer (G) smaller than P. Lets say they choose P=17 and G=14. It doesn't matter if anyone else discovers these numbers.
- They each pick a random number, x
- They each calculate G^x (mod P)
- They tell each other the result. Again it doesn't matter if anyone overhears this.

Diffie-Hellman key exchange

- Alice picks 5. She works out A = 14^5 (mod 17) = 12
- Bob picks 15. He works out B = 14^{15} (mod 17) = 11
- They tell each other the numbers (A & B)
- Alice can now calculate B^5 (mod 17) = 10
- Bob can now calculate A^{15} (mod 17) = 10

Diffie-Hellman key exchange

- Alice picks 5. She works out A = 14^5 (mod 17) = 12
- Bob picks 15. He works out B = 14^{15} (mod 17) = 11
- They tell each other the numbers (A & B)
- Alice can now calculate B^5 (mod 17) = 10
- Bob can now calculate A^{15} (mod 17) = 10

They have agreed on the number 10. No-one else could know this number, even if they were able to snoop on the entire conversation - unless they knew one of the original numbers (5 or 15), or were able to reverse 14^X (mod 17).

If much larger numbers were chosen, then reversing the calculation is almost impossible.

Public key cryptography

- An asymmetric algorithm
- You create two keys, a “public key” and a “private key”
- You can tell anyone your public key
- Anyone with your public key can use it to encrypt messages to you
- Messages encrypted using your public key can only be decrypted used the private key, that you have kept secret
- Secret keys are normally stored encrypted with a passphrase, to prevent unauthorised use even if people gain access to the computer storing them

RSA

- Rivest, Shamir and Adleman, 1977
- A public key algorithm
- Relies on the belief that there are no efficient algorithms to find the factors of large numbers

RSA

- Find two large primes: p & q
- Calculate $n = pq$
- Calculate e & d such that $ed = 1 \pmod{(p-1)(q-1)}$
- (e,n) can be published as your public key
- (d,n) can be kept as your secret key

It can be shown that $M^{ed} \pmod{n} = M \pmod{n}$

To encrypt a message M:

$C = M^e \pmod{n}$

To decrypt:

$M = C^d \pmod{n}$ since $C^d = M^{ed}$

Digital Signatures

- Public key cryptography allows the creation of digital signatures
- Alice encrypts a message with her secret key
- Anyone can decrypt the message using her public key
- Since they were able to decrypt the message, it must have been encrypted using Alice's secret key
- Only Alice has her secret key, so it must have been her that encrypted the message.

Message Digests

- A “digital fingerprint” for a message
- The message digest is generally much shorter than the message, typically 128 bits
- It should be impossible to work out the content of a message from it's message digest
- Given just a message digest it should be hard to create a message that would give the same message digest
- Given a message it should be hard to modify it without changing it's message digest
- Given these requirements it is not necessary to digitally sign an entire message, merely it's message digest.

Challenge Response Authentication

(based on a Message Digest Algorithm)

- The server sends the client a “nonce” that should be unique to this challenge
- Client concatenates the password with the nonce and calculates the digest of the result. This is sent to the server
- The server can then verify that the response from the client matches the version generated from the correct password
- Evesdroppers cannot obtain the password

Software

What software is there to enable us to use encryption easily and effectively to secure our communications?

HTTP digest auth

- Store the message digest (MD5) of the password on the server - prevents anyone breaking into the server obtaining the plaintext password (in case the user has used it elsewhere)

- Uses an MD5 based challenge-response mechanism to verify that the client knows the password (or rather the MD5 of the password, since that's what's stored on the server)

- Vulnerable to a man-in-the-middle attack, because the request can be modfied to send an HTTP basic authentication request to the client

SSH

- Allows secure remote login
- Used to access the Compsoc Linux boxes

- When you connect to an SSH server public key cryptography is used to allow secure communication
- Public key cryptography is slow, requiring a lot of processing power, so the server and client agree session keys, which are used with a symmetric encryption algorithm for all further communication
- The session keys may be changed periodically during the life of a connection
- SSH can optionally compress the stream before encrypting it

SSH – security features

- The client obtains the public key directly from the server, and tells you it's fingerprint – allowing you to verify this with the administrator if you wish. It records this key.
- If, during a later communication, the server attempts to use a different key the user is presented with a severe warning.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle
attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
ca:36:88:a6:68:e5:e4:25:70:18:20:cb:f1:33:0d:f3.
Please contact your system administrator.
```

SSH – security features

- Clients can have their own keys, produced using ssh-keygen
- The server can be configured to allow connections from certain client keys without asking or a password (normally configured using the “authorized_keys” file)

SSH – features

- SSH can be used to provide an encrypted tunnel for other TCP connections

```
ssh -L1110:localhost:110 the.remote.server
```

Will connect to the remote server and provide an encrypted tunnel for 'pop3' connections (which use port 110 by default). Connect your pop3 client to “localhost”, port 1110, and the data will be encrypted and sent over the SSH connection to the pop3 service on the remote server.

New versions of Putty include this functionality

PGP

- Normally used to encrypt or digitally sign email
- Can be used to encrypt other files for safe storage or transmission
- Public PGP keys are published on keyservers, and often also on people's web pages

PGP

- Normally used to encrypt or digitally sign email
- Can be used to encrypt other files for safe storage or transmission
- Public PGP keys are published on keyservers, and often also on people's web pages

Encryption process:

- File is compressed
- File is encrypted using a symmetric algorithm and a random session key
- Session key is encrypted using the recipient's public key. May be encrypted multiple times, once for each recipient.

PGP – Web of Trust

- Public PGP keys include the person's name and email address
- PGP keys can be digitally signed to say that they belong to the person named
- Anyone can sign a PGP key, though they should ensure that the key really does belong to the person claimed (for example by meeting the person and checking their passport and public key fingerprint)
- I can choose how much I trust signatures created by different people. By following chains of signed keys (starting with those I have signed) I can decide whether I trust a given key to belong to the person claimed or not

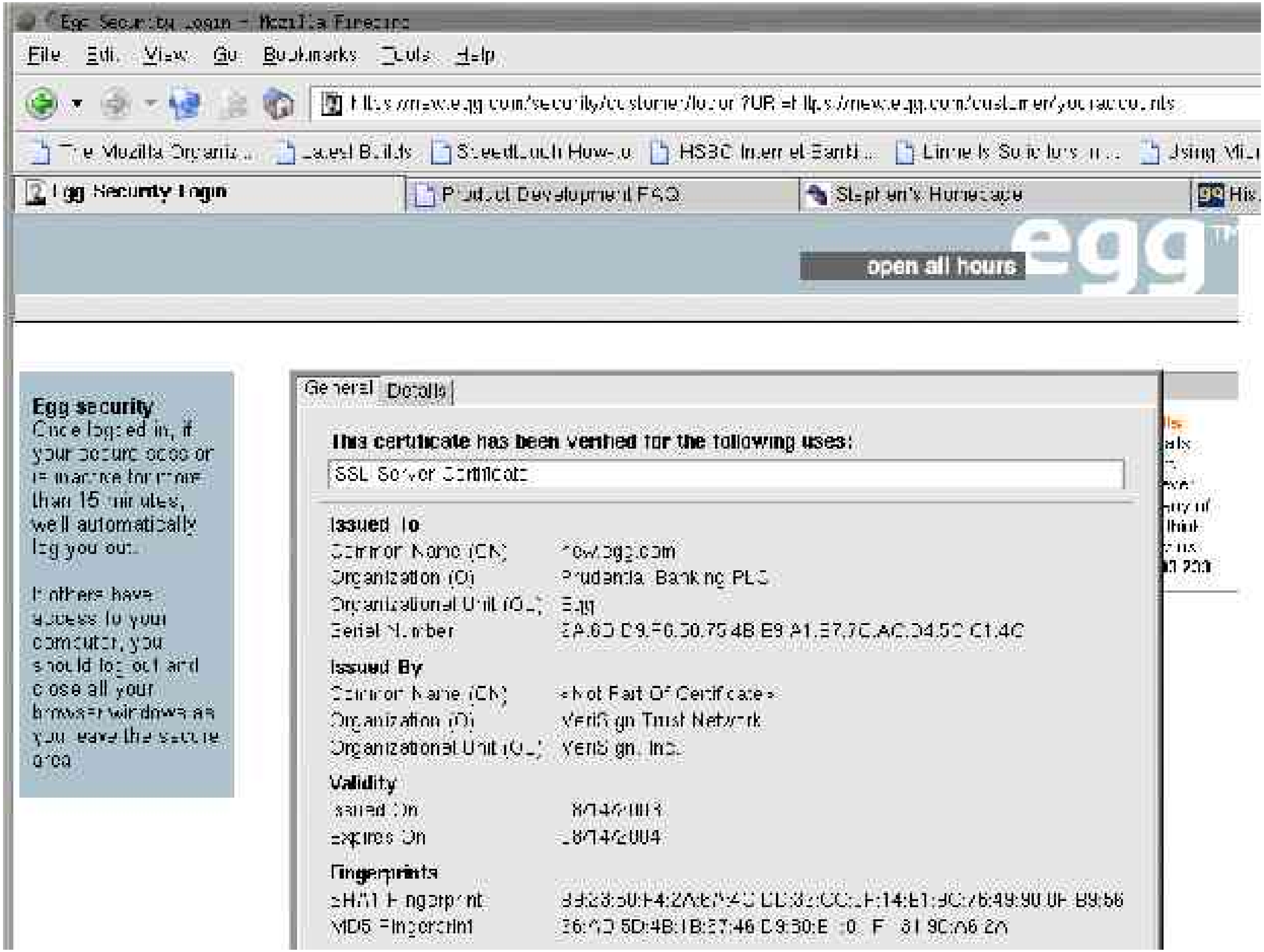
HTTPS

- Developed by Netscape when it was the dominant web browser
- The protocol has been generalised to produce “SSL”, which can be used to encrypt just about any stream (not just an HTTP connection)
- The cryptography involved is similar to SSH, PGP, etc.
- Like SSH, a client can obtain a server's public key directly from that server
- Like PGP, a public key contains information on who it belongs to and can be signed to verify this

HTTPS/SSL – Certificate Authorities

- A list of keys belonging to “Certificate Authorities” (CAs) are included in SSL client software
- Software automatically accepts any key signed by one of these authorities as valid
- Companies or individuals can pay the CAs to give them a signed public key
- This allows your web browser to verify the identity of the remote server, for example it can be sure that when you go to https://www.mybank.com/ that it really is talking to a server owned by mybank.com

HTTPS/SSL – Certificate Authorities


Egg Security Login - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://new.egg.com/security/customer/login?URL=https://new.egg.com/customer/youraccounts
The Mozilla Organiz... Latest Builds SpeedTouch How-to HSBC Internet Banki... Linux Is Solutions ... Using Mi...
Egg Security Login
Product Development FAQ
Stephen's Homepage
His...
open all hours
egg
General
Details

Egg security
Once logged in, if your secure session is inactive for more than 15 minutes, we'll automatically log you out.

If others have access to your computer, you should log out and close all your browser windows as you leave the secure area.

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To
Common Name (CN) new.egg.com
Organization (O) Prudential Banking PLC
Organizational Unit (OU) Egg
Serial Number 3A:6D:D9:F6:30:75:4B:E9:A1:37:7C:AC:04:5C:C1:4C

Issued By
Common Name (CN) <Not Part Of Certificate>
Organization (O) VeriSign Trust Network
Organizational Unit (OU) VeriSign, Inc.

Validity
Issued On 8/14/2003
Expires On 8/14/2004

Fingerprints
SHA1 Fingerprint 83:23:50:F4:2A:EF:4C:DD:32:CC:2F:14:E1:9C:76:49:90:0F:B9:56
MD5 Fingerprint 36:AD:5D:4B:1B:37:46:D9:30:E[illegible]:0[illegible]:F[illegible]:81:9C:A6:2A

SSL – other uses

- IMAPS and similar
- The public keys (X509 public key infrastructure) can be used for encrypted or digitally signed email, and this system (unlike PGP) is supported by default in Mozilla and Outlook Express
- It is possible to get personal keys, suitable for use in email clients, for free from one of the Certificate Authorities (Thawte) through a “Web of Trust” system

thawte
WEB
OF
TRUST
NOTARY

Virtual Private Networks

- Cryptography can be used to create VPNs
- To the user it looks like a private network between two locations
- In reality packets (data) are encrypted and sent over public networks (the internet) and decrypted at the far end
- Can be used to allow employees secure access to the company network from home
- Key distribution may not be a problem: a fast symmetric encryption algorithm is all that is required
- Modern systems can often use public private key cryptography, based on TLS and X509 keys

Virtual Private Networks

- OpenVPN
- IPSec

References

- The Code Book, Simon Singh
- http://www.ssh.com/support/cryptography/introduction/
- http://www.pgpi.org/doc/pgpintro/
- http://www.rsasecurity.com/rsalabs/faq/
- http://www.wikipedia.org/
- RFCs
- Lots of websites that forgot to write down, see google :)