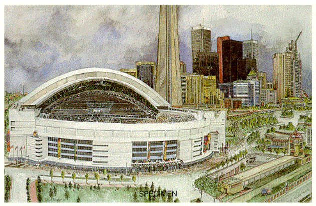
Cryptography

The Cryptic Puzzle

An Introduction To Cryptography



Ernest H. Nachtigall CISSP;CISA

IBM Canada

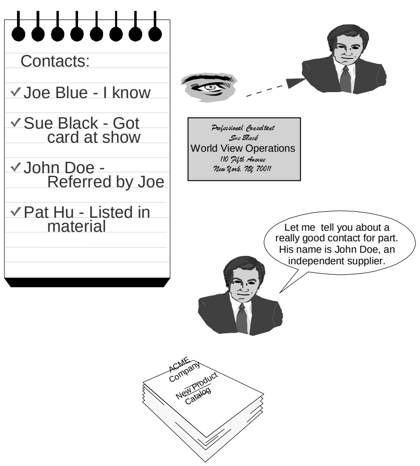
October 29, 1999

Old Business Done in New Ways

Cryptography

The Basics that Make Business Reliable

- Contacts
  - ✓ Recognition
  - ✓ Other Identifiers
- Information Exchange
  - ✓ Mail
    - Uncertified
    - Certified & Registered
  - ✓ Reports
  - ✓ Business Documents
  - ✓ Internal Documents

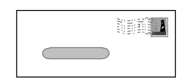


Cryptography

Exchange of Information

- Trusted Foundations
  - ✓ Established Linkages
  - ✓ Formal & Informal Structures
- Messages
- Reports
- Records
- Moneys

Canada Post



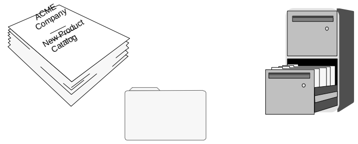
Privacy

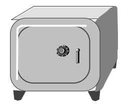
Established Trust

Linkage between Sender and Receiver

The BackBone of a Business

- Paper Trail
  - ✓ Proposal / Offering
  - ✓ Agreement of Sale
- Legal Issues
- Accountability Issues
- Accounts and Other Receivables

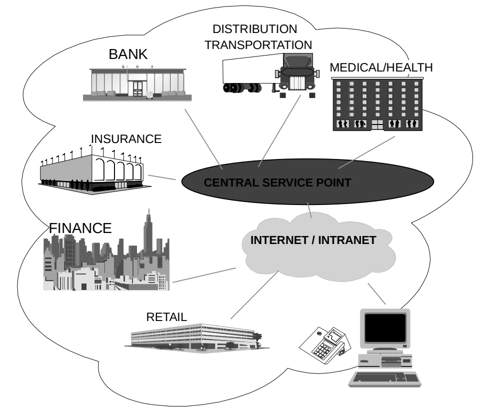




Exposures:
- Wiretaps
- Eavesdropping
- Data modification
- Authentication
- Non-proof of origin

The New Business Environment

- Moving towards a more "paperless" world
- World and business boundaries shrinking
- Growth demands quick response
- Need to match the emerging electronic media protocols



Enormous Possibilities Provided Public Confidence

Understanding Cryptography

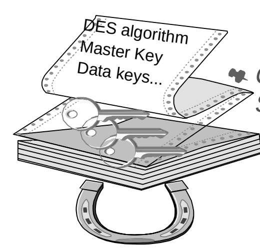
and

Cryptographic Functions

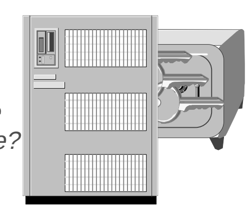
Cryptography - A Definition

Cryptography is the study of transforming information into a form that obscures its meaning.

- Most cryptographic systems consist of
  - ✓ a cryptographic engine(s) which performs algorithm(s)
  - ✓ keys
  - ✓ some cryptographic macros or APIs



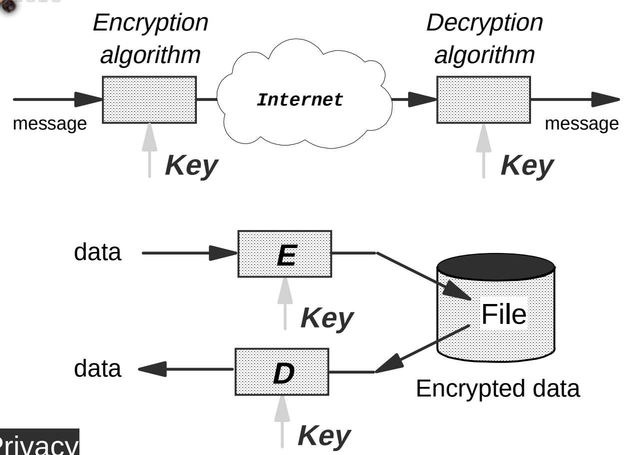
Cryptographic Engine
Software vs Hardware?



A matter of security...

Cryptography

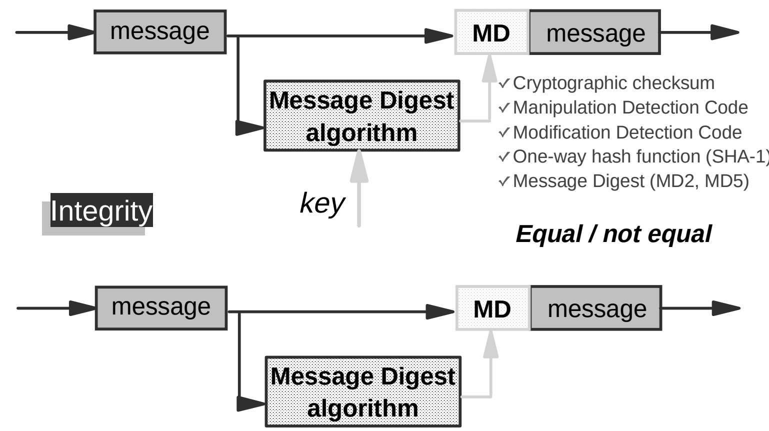
What is it? . . . Encryption



Privacy

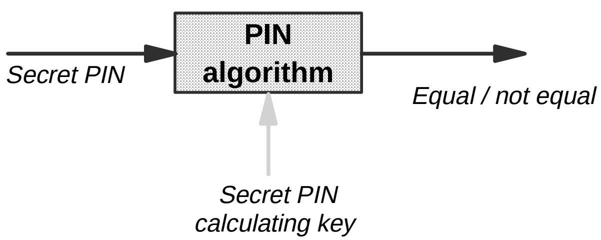
Cryptography

What Else? . . . Message Digests or Hashes



Cryptography

What Else? . . . PINs

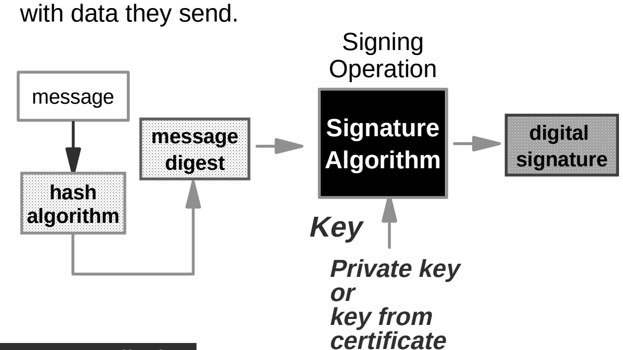


Authentication

Cryptography

What Else? . . . Signatures

Signatures are a way to securely associate someone with data they send.



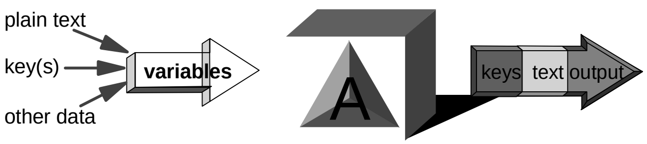
Non-Repudiation

Authentication

Cryptography

Cryptographic Algorithms

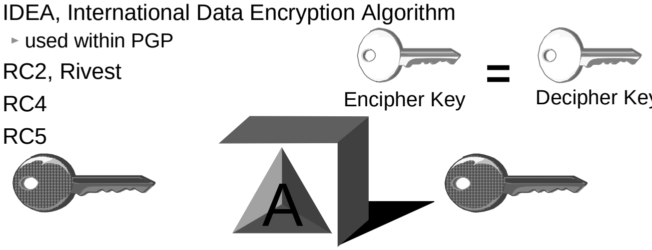
- Formula used to transform the plain data or readable text into cipher text or encrypted text
- Key is the mechanism that makes the output of the formula different from other output
- Algorithms can sometimes have other variables as input to further distinguish the output of the formula



Cryptography

Symmetric Algorithms

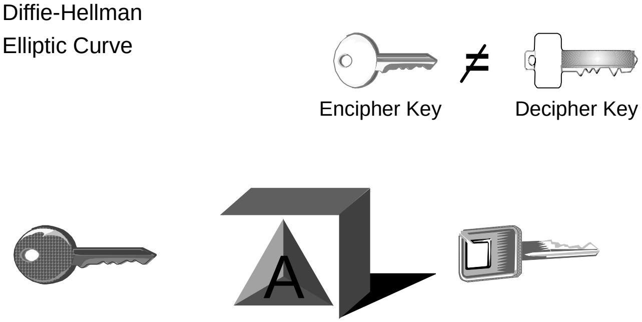
- Characterized by identical key values in key pair generation
- Examples:
  - DEA or DES, Data Encryption Algorithm or Data Encryption Standard
  - Triple-DES, DES but using 3 key values rather than 1
  - CDMF, Common Data Masking Facility
  - IDEA, International Data Encryption Algorithm
    - used within PGP
  - RC2, Rivest
  - RC4
  - RC5



Cryptography

Asymmetric Algorithms

- Characterized by unique key values in key pair generation
- Examples:
  - RSA, Rivest Shamir and Adleman
  - Diffie-Hellman
  - Elliptic Curve



Cryptography

Keys

- String of hexadecimal numbers which can be entered as alphanumeric characters
- Symmetric keys are usually 8-bytes in length with the high-order bit serving as a parity bit. (8x8 = 64-8 = 56 bits)
- Asymmetric keys are usually 128-bytes in length or 1024-bits
- Example of single length DES key
  - 332137D1, hex value of x'F3F3F2F1F3F7C4F1'
- Keys are sometimes protected under a host secret key called a Master Key

Cryptographic Algorithms: A Cipher Sample

Cryptographic algorithms create a restructuring of data

- ciphering of a clear key value (K) to produce an enciphered key K_{KM}

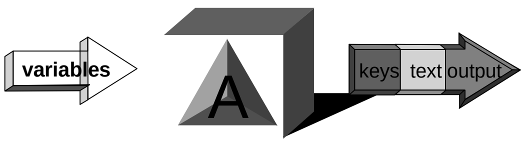
332137D1 ⇨ A ⇨ 82F267C50956E and looks like ⇨ ê /&|Pòn

- ciphering of clear text value to produce ciphertext

PAY ERNIE NACHTIGALL $100.00 AUTHORIZED BY N.LEE

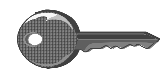
u ╥#[& ╡cO£ôd a : ┼○ X÷ í||ò└ ┴i' ÁJ ø ⁒ § [+⊥ î∞ â
"*5

- using input variables

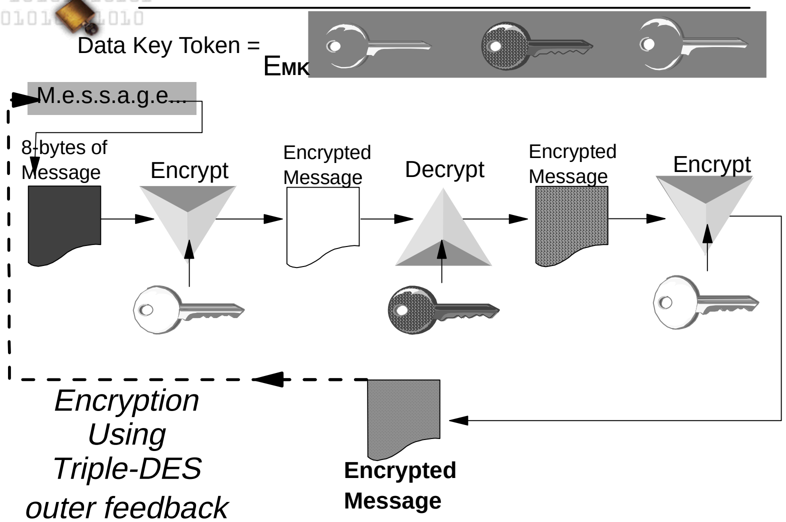


Key Lengths

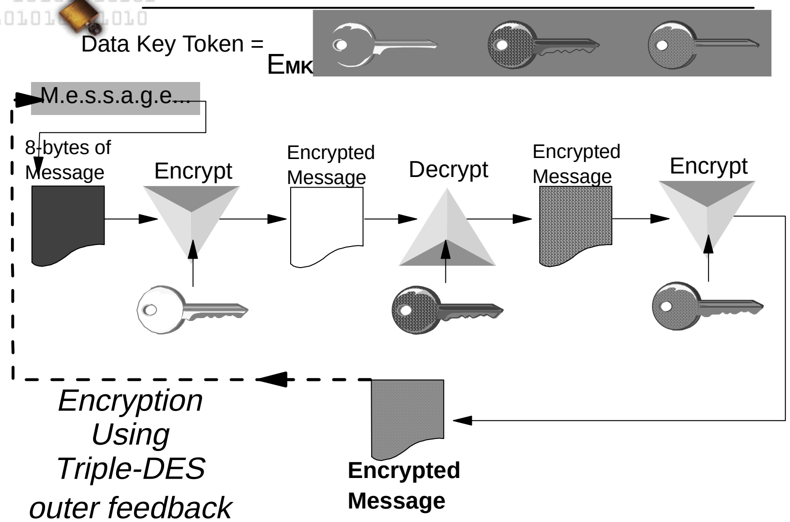
- Key lengths are export controlled depending on the key function
- For encryption
  - 40-bit lengths are exportable
  - 56-bit lengths are exportable under special agreement
  - 128-bit and longer are export controlled
- For digital signature generation and verification
  - 512-bit and 1024-bit is exportable
  - longer strings are export controlled
- For key distribution
  - 512-bit is exportable
  - longer strings are export controlled



Triple-DES Processing : Overview . . .



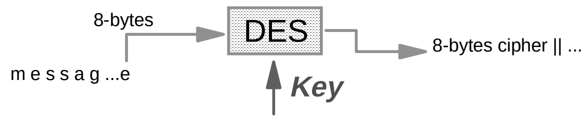
Triple-DES Processing : Overview



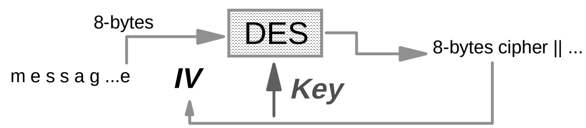
Cryptography

DES Basic Modes of Operation

- Electronic Code Book (ECB)
  - basic block encryption of 8-bytes (64-bits) at a time



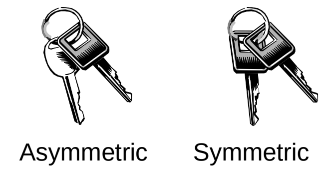
- Cipher Block Chaining (CBC)
  - encrypts 8-bytes at a time
  - uses an initialization vector to XOR with first 8-byte block, each subsequent 64-bytes of message are XORed with previous

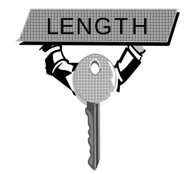


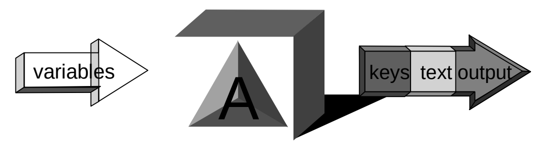
Cryptography

Basic Crypto Mechanisms

- Encryption/Decryption
  - Algorithms
  - Key Lengths
- Hashes and Digests
  - SHA-1 and MD5
  - Message Authentication
  - Modification Detection







Cryptography

Basic -> Complex Mechanisms

- Random Number Generation
  - Pseudorandom number generator (PRNG)
  - Seed value calculated
    - differently each time, or
    - using an internal state
- Personal Identification Number Functions
  - Algorithms
  - Tools for authentication
  - Various functions use simple basic crypto functions and a combination of crypto functions

Cryptography

Complex Mechanisms: Signatures & Certificates

- Signatures
  - Algorithms
    - ANSI X9.30 - Digital Signature Standard
    - ISO 9796 - Rivest Shamir and Adleman
    - RSA DSI PKCS 1.0 & 1.1
  - $e_{\text{private key}}$(Hash)
- Certificates
  - X 509.3
  - Hashing + Signatures

The Algorithms

DES

PKA

Cryptography

Public Key Cryptography

- Mathematically related key pair
- Very large prime numbers over 100 digits long

– Generate 2 prime numbers	P = 7 Q = 17
– Multiply the prime numbers	7 x 17 = 119 = N
– N is first part of Public Key	Public Key 119 E
– N is first part of Private Key	Private Key 119 D
– Select odd number; this is second part of public key	Public Key 119 5
– Second part of private key =	(7-1)x(17-1)x(5-1) = 384
(P-1) x (Q-1) x (E-1)	(7-1) x (17-1) x (5-1) = 384
Add 1 to result	384 + 1 = 385
Divide by E = D	385/5 = 77 = D
.	Private Key 119 77

- Convert characters to numeric
  - eg. a=1, b=2, c=3.....
  - SELL becomes 19 5 12 12

Cryptography

Encipher Message

- P = 7; Q = 17; N = 119; E = 5; D = 77
- Public Key = N E = 119 5
- Private Key = N D = 119 77
- Convert characters to numeric
  - eg. a=1, b=2, c=3.....
  - SELL becomes 19 5 12 12
- Character raised to power E — "S" = 19; 19**5 = 2476099
- Divide by first part of Public Key Remainder is enciphered character — 2476099 / 119 = 20807 and remainder 66 = eKP(S)

Cryptography

Decipher Message

- P = 7; Q = 17; N = 119; E = 5; D = 77
- Public Key = N E = 119 5
- Private Key = N D = 119 77
- a=1, b=2, c=3.....
  - SELL becomes 19 5 12 12
- Character raised to power E
- Remainder raised to power D — 66 ** 77 = 1273.......
- Result divided by first part of Private Key and Public Key — 1273..... / 119 = 1069 and remainder of 19
- Remainder is numeric equivalent of character sent — 19 = "S"

Cryptography

A Simple HASH Function

- Text 1 = 1234567890000000
- Text 2 = 0987654321000000
- DES Key A = 0101010101010101
- DES Key B = 0123456789ABCDEF
- Encrypt Text 1 with Key A — CEAA B413 9FA4 CF0B
- EXOR result with Text 2 — C72D D150 BEA4 CF0B
- Encrypt result with Key A — 844F 04B9 424D 04AB
- Decrypt result with Key B — ED31 0574 90F9 85DD
- Encrypt result with Key A — CB50 5EE4 6F6E 331B
- Select (left to right) numerics. Select (left to right) alpha, and decimalize.

Cryptography

A Simple HASH Function

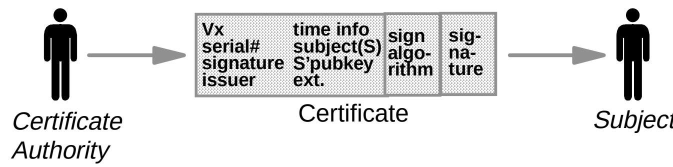
- Text 1 = 1234567890000000
- Text 2 = 0987654321000000
- DES Key A = 0101010101010101
- DES Key B = 0123456789ABCDEF
- Encrypt Text 1 with Key A — CEAA B413 9FA4 CF0B
- EXOR result with Text 2 — C72D D150 BEA4 CF0B
- Encrypt result with Key A — 844F 04B9 424D 04AB
- Decrypt result with Key B — ED31 0574 90F9 85DD
- Encrypt result with Key A — CB50 5EE4 6F6E 331B
- Select (left to right) numerics. Select (left to right) alpha, and decimalize.
- **5054 6633 1214 4541**

Certificates and Such

Cryptography

Certificates

Certificates are a way of securely identifying someone.
Most are based on the standard structure X 509 v3.



Authentication

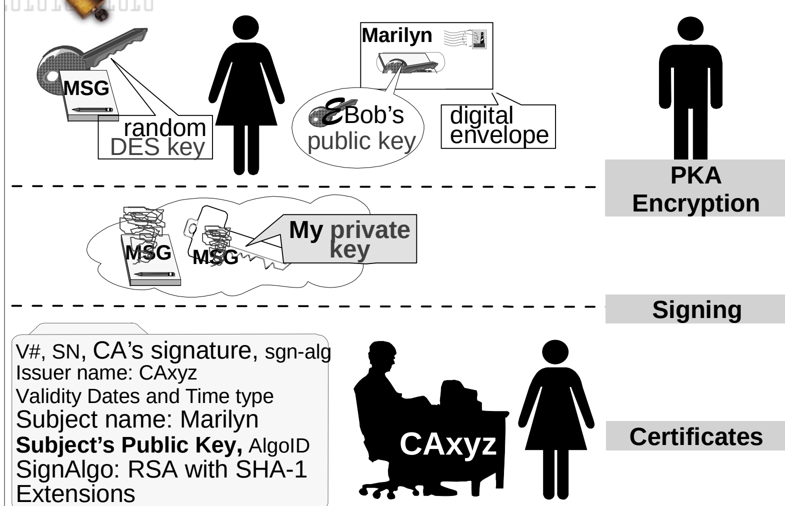
Cryptography

Certificate Basics

- There are many variations of certificates.
- Certificate Authorities also vary.
  - Entrust,
  - Verisign, etc...
  - even you can have a certificate authority within your enterprise
- Certificate Authority (CA)
  - Trusted Third Party
  - Responsible for establishing basic trust
    - serve to validate the identity of the certificate subject and the subject's association with the public key material within certificate
    - signs the data representing info about the subject
- Certificate Repository
- Certificate Revocation List (CRL)
  - notification of change

Cryptography

Complex Ideas: Signatures & Certificates



What to do with Certificates

- How are they to be used?
- Define Policy based on use
  - what CAs to be used
  - what CAs to support
  - what type certificates to support
  - how often to get CRLs and from where
  - other specific certificate related data
  - backup and storage rules
- Check to see which installed vendor products use certificates

What to do with Certificates . . .

- Authentication
  - must verify the received certificate
    - check the signature of the CA issuing the certificate
    - check the most recent revocation list as defined by your policy
- Determine how to obtain end user public-private key pair
- Algorithms required
  - SHA-1, MD2, and MD5 for performing one-way hash functions
  - RSA PKCS#1 and DSA for processing digital signatures
  - RSA, DSA, and Diffie-Hellman for manipulating public keys
- Most vendor products using certificates handle these issues within the product code

Cryptography for Network Security

Complex Mechanisms: SSL & SET

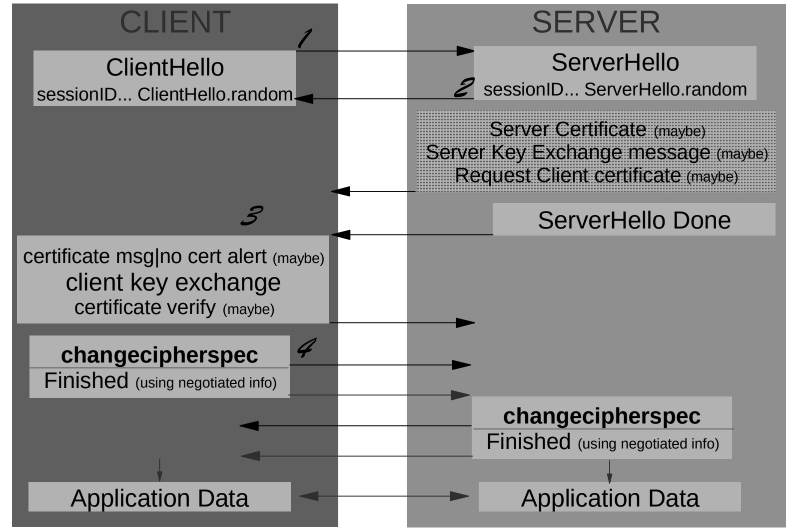
- SSL
  - authentication via SSL handshake protocol
  - connection privacy via SSL record protocol
- SET Protocols
  - e-Commerce with Trust
  - describes 'rules of conduct' and uses all forms of cryptographic mechanisms
  - interfaces with traditional structure

Cryptography

Secure Sockets Layer (SSL)

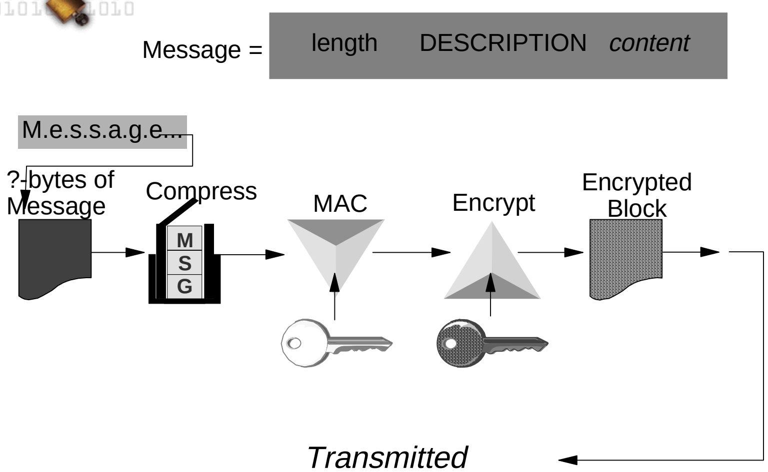
- SSL is a standard protocol which help define the "rules of conduct" between the two entities wishing to communicate.
- There is a handshake level of security and a record level security.
- Within the protocol are various implementations of cryptographic functions which when used as defined by the protocol provide the security.
- SSL uses
  - random numbers
  - hashes
  - PKA algorithms
  - DES encryption
  - digital signatures

SSL Handshake Processing : Overview



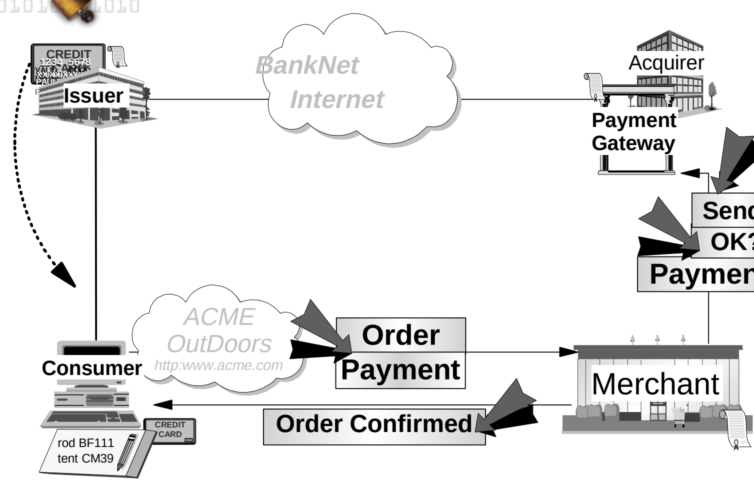
Cryptography

SSL Protocol Processing : Record Layer



Cryptography

SET Processing : Overview



Complex Mechanisms: IPSEC

- IP Authentication Header (AH)
  - Provides integrity and authentication without confidentiality
  - MD5 algorithm using a 128-bit key, at a minimum
  - Hash for the packet's contents
- IP Encapsulating Security Payload (ESP)
  - Provides confidentiality, and might also provide integrity and authentication
  - Encapsulates either
    - an entire IP datagram or
    - the upper-layer protocol data inside the ESP and appends a new cleartext IP header to the encrypted ESP
  - Tunnel-mode
  - Transport-mode
  - Encrypt packet data contents

Mix N' Match

Using Cryptography across Systems

Export Issues

- US Commerce has relaxed controls on cryptography, granting permission to ship stronger encryption within products based on key recovery.
- CMOS Cryptographic Coprocessor which is standard on G4+ Servers and Application StarterPak systems is <u>not export controlled</u>. The hardware is not enabled at shipment.
- Enablement Diskette is <u>export controlled</u>. It activates the hardware.
- ICSF is <u>not export controlled</u>.

Export Controls

Crypto export control is concerned with encryption strength. This is directly related to key length and purpose.

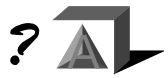
Since January 1, 1997, export of 56-bit encryption products is allowed if a company agrees to implement key recovery technology in the products in a future release.

128-bit encryption can only be exported to financial institutions and used solely for financial applications, the first of these being home banking.

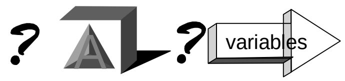
Encryption algorithms, RC2 and RC4 from RSA Data Security, are used by Netscape and Microsoft, for home banking applications. The applications will make use of 128-bit encryption when connected to a bank server. Netscape and Microsoft will use special digital certificates (from Verisign) in their bank servers, which will be recognized by their respective browsers. Upon validation that the special certificate is present, thereby authenticating connection to a proper bank server, the browser will allow 128-bit encryption to be enabled specifically for the banking application. If the special certificate is not present, then the browser reverts back to 40-bit encryption capability. The 128-bit encryption capability can not be used for general purpose encryption.

Cryptographic Sharing Across Systems

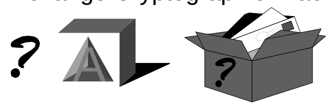
- Exchange Keys



- Exchange Cipher Text

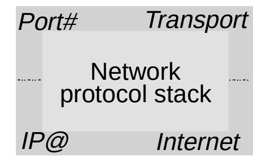


- Exchange Cryptographic "Package"

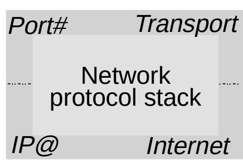


Firewalls & Web Servers

- Web Servers
- Purpose is to provide access to data
  - Many browsers incorporate SSL within their code
  - Allows security via authentication and privacy
  - Integration of SSL protocol code within applications
  - The web server can perform SSL tunneling.
  - It is the browser which provides the encryption for the client workstation.



Firewalls & Web Servers . . .

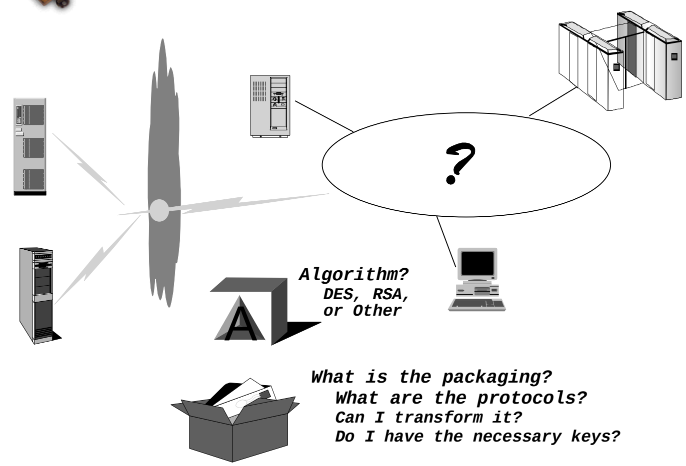


- Firewalls
- Purpose is to control the flow of traffic
  - Prevent exposure of IP addresses
  - Prevent certain untrusted entries into environment
  - Prevent certain flows outbound from within environment
  - Firewalls when communicating with one another can use SSL tunneling.

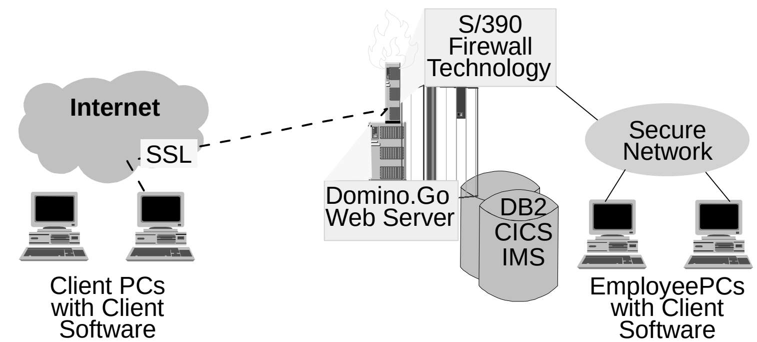
Application Crypto Use

- Must have a cryptographic engine either hardware or software
  - BSAFE
  - CMOS Crypto Coprocessor
- Must code the required calls to perform the crypto functions desired
  - BSAFE
  - Integrated Cryptographic Services Facility (OS/390 V2)
- Must obtain keys/certificates for use
  - Crypto engine
  - Certificate Authority
- Must interoperate based on established protocols with other systems
  - SSL, SET, IPSEC, etc.

Mix N' Match

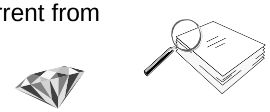


Web Support

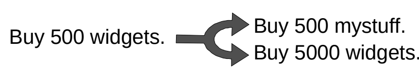


Cryptographic Value

- Confidentiality, protection and deterrent from
  - theft, unauthorized copying
  - unauthorized viewing



- Data Integrity/Modification
  - fraud
  - theft



  - malicious and unintentional loss by deception
  - proof of originality
- Digital Signature
  - proof of authorship
  - legal satisfaction

- Authentication
  - proof of identity

Questions?

enachtig@ca.ibm.com Phone 1.416.410.5909