Vanguard Security and Compliance 2012

Session AST1: Cryptography 101: Acronym Soup

Speaker Name: Ernest Nachtigall **CISSP;CISA**

IBM Canada

THE Open GROUP Master Certified IT Specialist

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Introduction to Cryptography

- What is cryptography?
- Why cryptography?
- Cryptography & main use

What is Cryptography

- **Cryptography** (or cryptology; from Greek κρυπτός, *kryptos*, "hidden, secret"; and γράφω, *gráphō*, "I write", or -λογία, *-logia*, respectively) is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering.

From Wikipedia

Cryptography

- "Secret Writing"
- The practice and study of hiding or securing information
- Currently closely aligned with mathematical theory

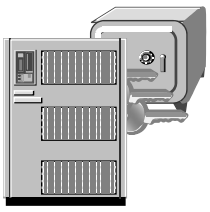
Cryptography – In Perspective

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 versus Hardware?*

A matter of security...



Identifying The Problems

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- California SB 1386
- Gramm-Leach Bliley Act (GLB)
- Sarbanes-Oxley (SOX)
- **Payment Card Industry (PCI)**

VISA CISP

- VISA introduces Cardholder Information Security Program June 2001
  - Designed to assist merchants in providing secure transaction processing, protecting customer data
- VISA, MasterCard, American Express, Discover, JCB combine to draft **PCI-DSS** Sept 2006
- Compliance mandatory June 2007

Cryptographic Standards

- CCA (Common Cryptographic Architecture)
- PKCS (Public-Key Cryptography Standards)
- INTEL CDSA (Common Data Security Architecture)
- ANSI (American National Standards Association)
- ISO (International Organization for Standardization)
- FIPS (Federal Information Processing Standards)

The Need

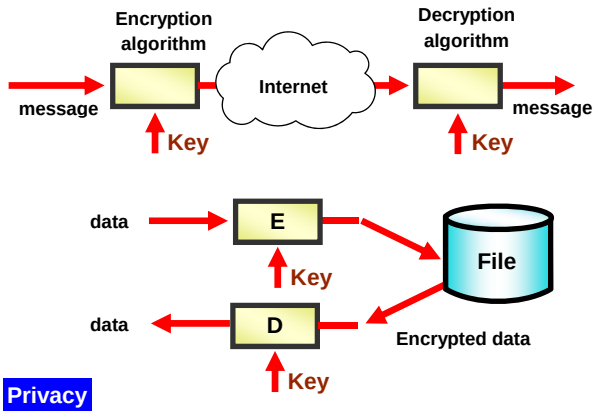
- Traditionally: to hide the meaning of transferred or stored data, but also used to establish:
  - Data confidentiality (Not disclosure)
  - Data integrity (No alteration)
  - Authentication (Identity Verification)
- A required facility today for personal or industrial computing
- Hardware Cryptography
  - Offload cryptographic computation workload
    - Some algorithms consumes huge amounts of MIPS
  - Increased performance
    - Speed of computation by specialized coprocessors
  - Security
    - Always more secure than a software implementation
    - Can implement very sophisticated protection of secrets, depending on device

What **CAN** Encryption Do?

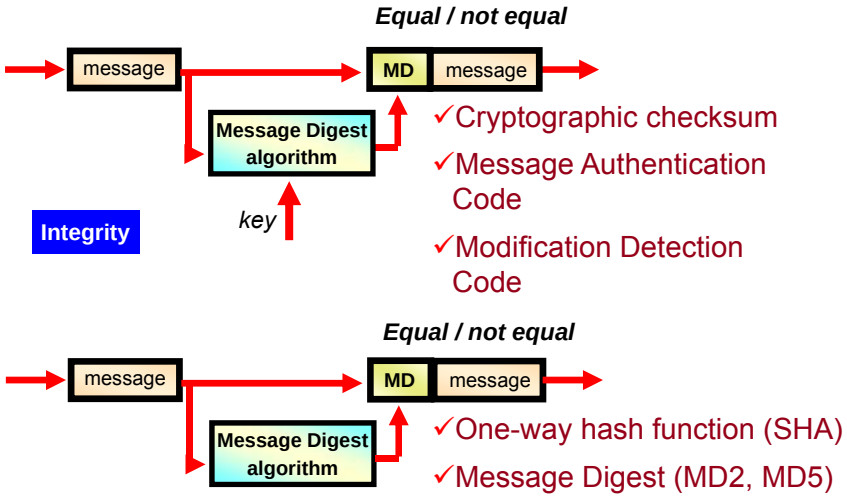
- Encryption / Decryption
  - **Privacy** - To protect the contents of data from others
- Message Digests and Hashing
  - **Data Integrity** - To allow verification that data is received was the same as the data that was sent
- Personal Identification Numbers
  - **Identification** - To associate a person with data/objects based on knowledge they have and that is associated with that data or object.
- Proof of Origin (**non-repudiation**)
  - Digital Signatures

.

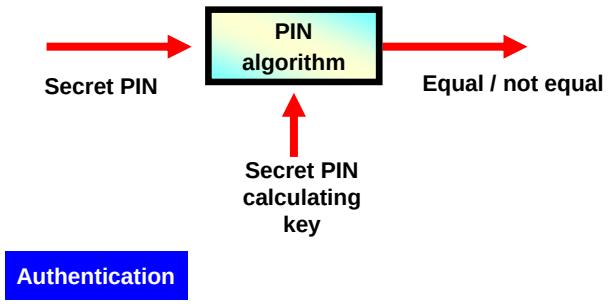
What is Cryptography? Encryption



What Else? Message Digests or Hashes

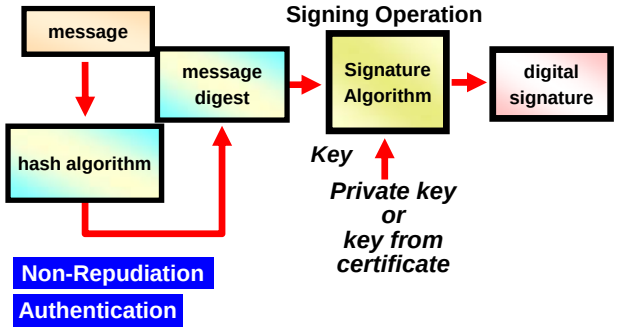


What Else? PINs



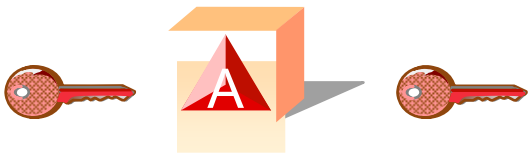
What Else? Signatures

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



Symmetric (Secret Key) Algorithms

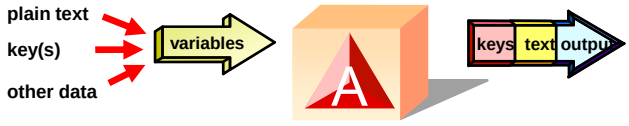
- **Secret Keys** characterized by identical key values in key pair generation
- Examples:
  - **Block Ciphers**
    - DEA or **DES**, Data Encryption Algorithm or Data Encryption Standard
    - **Triple-DES**, DES but using 3 key values rather than 1
      - NIST says good until 2030
    - **IDEA,** International Data Encryption Algorithm (used in PGP)
    - **RC2**
    - **AES**
  - **Stream Ciphers**
    - **RC4**
    - **One Time Pad**



March 2001

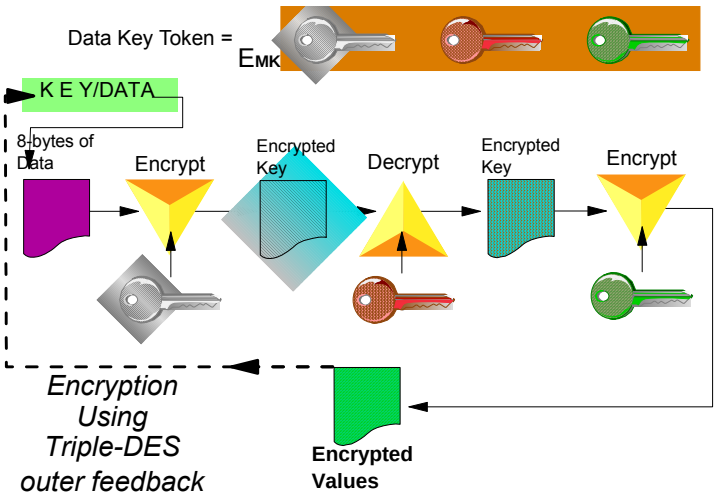
Cryptographic Algorithms

- Formula used to transform the plain data or readable text into cipher text or encrypted text
- Formulas well documented so a key is the mechanism that makes the output of any formula different from other output of the same formula
- Algorithms can sometimes have other variables as input to further distinguish the output of the formula



March 2001

Data Confidentiality – Why TDES



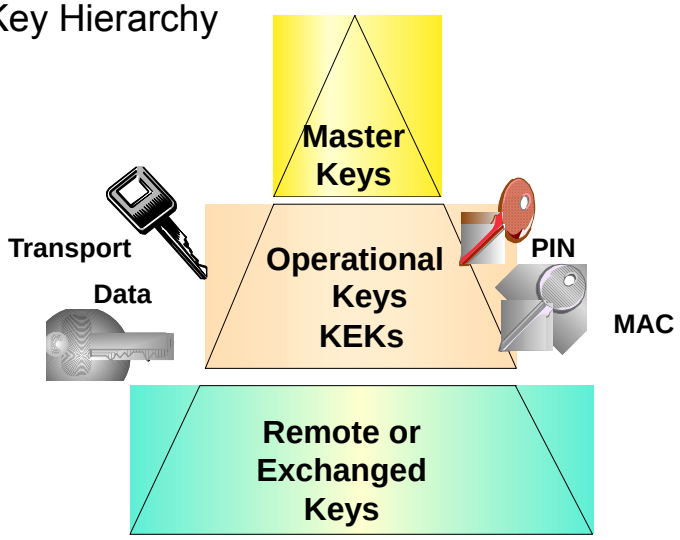
Rijndael (AES)

- Named after its creaters, two Belgian cryptographers, Joan Daemen and Vincent Rijmen
- AES - Advanced Encryption Standard
- 128 bit key 3.4X10**38 (340 Undecillion)
- 192 bit key 6.2X10**57 (6.2 Octodecillion)
- 256 bit key 1.1X10**77 (almost a Googol)
- Given 2**55 DES cycles per second (recover any key in 1 second)
- 149 trillion years to recover 128 bit AES.
- Web Site http://csrc.nist.gov/encryption/aes/

Keys

- String of hexadecimal numbers which can be entered as alphanumeric characters
- Symmetric keys are usually 8-bytes in length with the high-order bits 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'
  - or 3AK2P7D1, hex value of x'F3C1D2F2D7F7C4F1'
- Keys are sometimes protected under a host secret key called a Master Key

DES Key Hierarchy



Clear Key vs Encrypted (Secure) Key

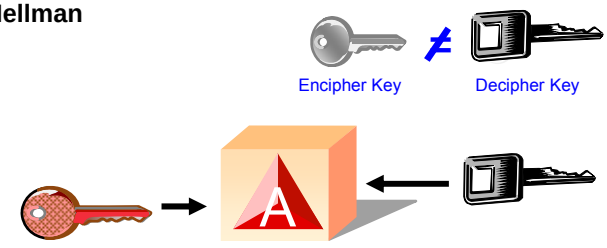
- Clear Key
  - C'TESTKEY1' or X'E3C5E2E3D2C5E8F1'
  - **SPEED! (40X-100X)**
  - SSL, Encryption Facility, DB2/IMS Encryption
- Encrypted (Secure) Key
  - e_{mk}(TESTKEY1) = X'C7E24CA92F4AB03E'
  - e_{kek}(TESTKEY1) = x'76B5C7EF973267CC'
  - **ADITIONAL SECURITY**
  - ATM, POS, PIN

Performance vs. Strong Security

- Hardware Cryptography
  - Offload cryptographic computation workload
    - Some algorithms consume huge amounts of MIPS
  - Increased performance
    - Speed of computation by specialized coprocessors
  - Security
    - More secure than a software implementation
    - Can implement very sophisticated protection of secrets, depending on device

Asymmetric Algorithms

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



Asymmetric Key Usage

- **Private Key** is used for functions required to confirm ownership or origin
  - Signature, my signature = my private key
  - My private is not shared, only I could have produced signature


Private Key

- **Public Key** is used for functions required to maintain privacy or ensure understanding by a single person
  - Encryption, data with public key of Ernie
  - Only Ernie can decipher data


Public Key

- **Digital Signature** Processing
  - Private Key used to create Signature
- **Symmetric Key** Distribution
  - Public Key used to encrypt key value

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 (Modulus) — **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 (Exponent) — **Public Key 119 5**
  - Second part of private key = (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 — **Private Key 119 77**
- Convert characters to numeric
  - e.g.. a=1, b=2, c=3.....
  - SELL becomes 19 5 12 12

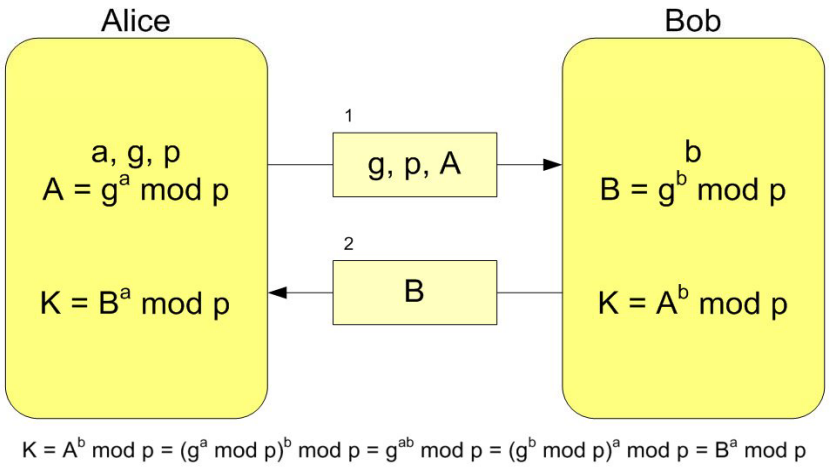
Encipher Message

- 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
  - e.g.. 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 2476099 / 119 = 20807 and Remainder is enciphered character remainder 66 = eKP(S)

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 1273..... / 119 = 1069 and Public Key remainder of 19
- Remainder is numeric equivalent 19 = "S" of character sent

Diffie-Hellman



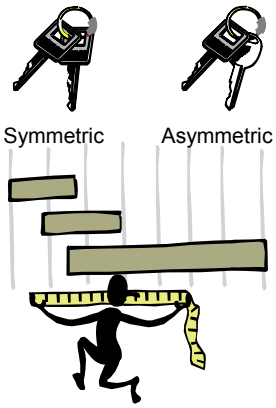
$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Diffie-Hellman

Alice	Bob
p prime	p prime
g generator < p	g generator <p
$A=g^a \bmod p$	$B=g^b \bmod p$
generate a	generate b
exchange $g^a \bmod p$ (A)	exchange $g^b \bmod p$ (B)
calculate $g^{ab} \bmod p$	calculate $g^{ba} \bmod p$
$g^{ab}=g^{ba}=K$	$g^{ab}=g^{ba}=K$

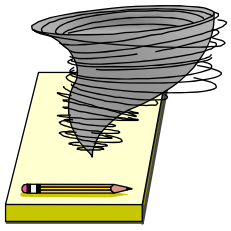
Basic Crypto Mechanisms

- Encryption/Decryption
  - Algorithms
  - Key Lengths
- Hashes and Digests
  - **SHA-1 SHA-256** and **MD5**
  - **Message Authentication (MAC)**
    HMAC
  - Modification Detection



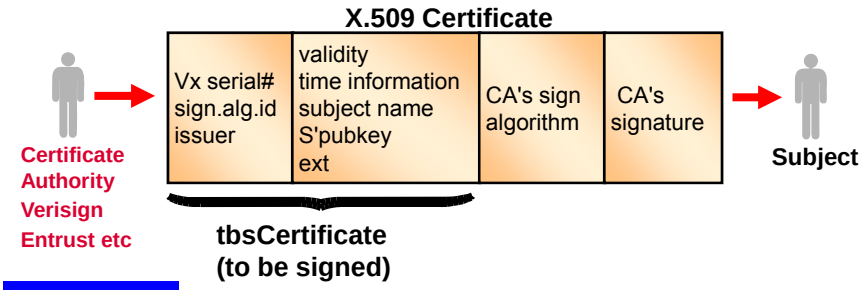
Complex Mechanisms: Signatures and Certificates

- 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



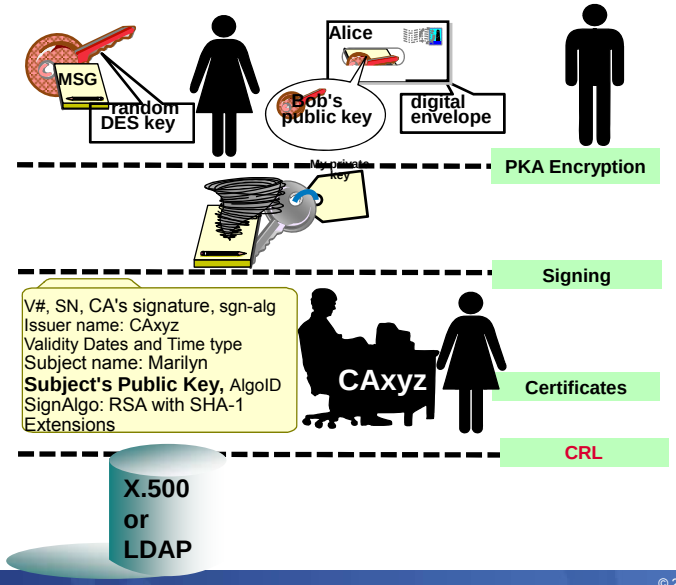
Certificates

- Certificates are a way of securely identifying someone. Most are based on the standard structure X.509 v3
- Certificates are encoded using DER rules (X.209)
- ASN.1 (Abstract Syntax Notation)DER encoding is a tag, length, value encoding system for each element.



Authentication

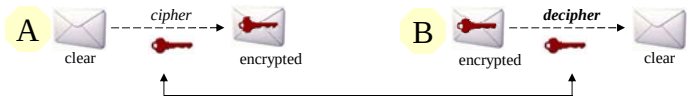
Complex Ideas: Signatures and Certificates



Reminder: Encryption of data

- **Symmetric encryption**

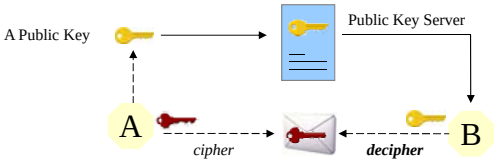
Confidentiality



- **Asymmetric encryption**

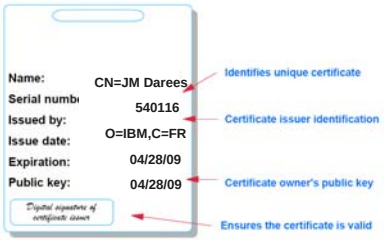
Confidentiality

Authentication



Reminder: Public Certificate

- Digital document that gives evidence that a public key belongs to whom it may concern. It contains at least the information listed below
  - Public Key
  - Certificate owner's Identity
  - Expiration Date
  - Signature from a third party
  - An utilization type

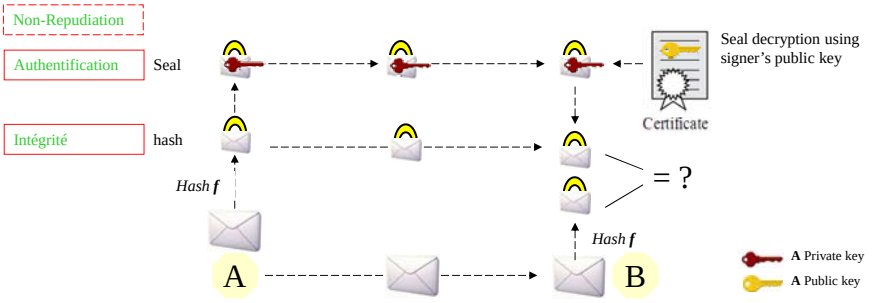


- Data which can be manipulated by computers
- Based on a norm : X509
  - Universal understanding and utilisation

Reminder : Hash & Digital signature

- **Hash function** is any well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serve as an index to an array. The values returned by a hash function are called hash values, hash codes, hash sums, checksums or simply hashes.

- A **digital signature** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit.



Cryptographic Algorithms and their main use

> **Symmetric algorithms (Shared Secret Key)**
Confidentiality of data

DES (56 bits)
T-DES (168 bits)
AES (128 bits)
*** AES (192, 256 bits)**

Data transfer (VPN, SSL/TLS, ..)
Data storage (database, archives, …)

ECC (New)
RSA (512, 1024, 2048, 4096 bits)
DSA (512, 1024 bits)

Authentication, key distribution
(VPN, SSL/TLS handshake, ..)

Private
Public

> **Asymmetric algorithms (Public Key Cryptography)**
Digital signature
Confidentiality of key

> **Cryptographic "checksum" with one way algorithms**
Integrity of data

Performed in hardware in System z10 EC/BC

MD5 (128-bit hash)
MAC, MDC
SHA-1(160-bit hash)
SHA-256 (256-bit hash)
SHA-384 , SHA-512

Data transfer (VPN, SSL/TLS, ..)
Data storage (database, archives, …)

Some Cryptographic Best Practices

- Multi custody of keying material
- Key custodians from separate business areas
- Change keys on a scheduled basis
  - Or upon suspected compromise
  - Or termination of key custodian(s)
- Unique key per device
- Backup copies of keys
- DR testing, hardware validation
- DES use of double or triple length keys
- AES 256 bit
- HASH alone is not secure
  - MAC using shared secret keys or Signatures

Some Cryptographic Best Practices…

- Do not knowingly reuse keys
- Force key separation
  - Unique MAC, DATA, PIN
- Do not encrypt everything with the same key
  - Use expiry date MMYY?
    - Credit Card issue cycle is 3 years
    - 36 MMYY per cycle
    - 36 PIN, CVV/CVC, CVV2/CVC2 keys
- Protect PIN DECimalizationTABle

References

- ATS TechDocs Web Site
  - http://www-1.ibm.com/support/techdocs/atsmastr.nsf
    - search on CRYPTO
- IBM Web Libraries
  - http://www-1.ibm.com/servers/eserver/zseries/zos/bkserv/
  - http://www-1.ibm.com/servers/eserver/zseries/library/online_pubs.html
  - http://www-1.ibm.com/servers/eserver/zseries/library/whitepapers/
  - http://app-06.www.ibm.com/servers/resourcelink
  - http://publib-b.boulder.ibm.com/Redbooks.nsf/RedpaperAbstracts/redp3747.html?Open
- Standards
  - http://www.ietf.org/
  - http://csrc.nist.gov/cryptval/140-1/1401val.htm
  - http://www.rsasecurity.com/rsalabs/standards/
- Free Stuff
  - http://www/infosecuritymag.com
  - http://www.scmagazine.com/index2.html
  - http://www.schneier.com/crypto-gram.html
  - http://www.simonsingh.net/The_CDROM.html

Crypto Class 1.5 + 3.5 Days

- ICSF Install and Crypto Components (lecture)
- ICSF Crypto Application Programming (TSO calling to ICSF)

- NO CHARGE!
- enachtig@ca.ibm.com

Questions

Programming can be fun, so can cryptography; however they should not be combined.

--Kreitzberg and Shneiderman