Crypto Concepts

Understanding the Buzz Words
SecureWorld Session I01

Marilyn Frazier Allmond
Advanced Technical Support
Washington System Center

S/390 zSeries Crypto Hardware, ICSF, and TKE
allmond@us.ibm.com

Trademarks and Other Stuff

- RSA and BSAFE are Trademarks and Registered Trademarks of RSA Data Systems
- Sites of Interest
  - **Standards from IETF at http://www.ietf.org**
    - **http://www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-05.txt**
    - **http://www.ietf.org/html.charters/pkix-charter.html**
    - **ftp://ftp.isi.edu/in-notes/rfc2459.txt**
  - **SSL**
    - **http://home.netscape.com/eng/ssl3/ssl-toc.html**
    - **ftp://ftp.isi.edu/in-notes/rfc2246.txt**
  - **ATS Technical Documents**
    - **This presentation will be placed on-line at the URL below within the next 2 weeks. Find it by using SEARCH ALL DOCUMENTS and keywords "crypto SecureWorld"**
    - **http://www-1.ibm.com/support/techdocs/atsmastr.nsf**

Buzz Word Central

- What is Cryptography
- "Packaging"
- Basics of Algorithms and such
- Basic Cryptography Functions
- Complex Stuff like Certificates

What is Cryptography?

- Transformation of readable, understandable data to a form that is not
- Transformation is based on a mathematical formula
- There are formulas for the transformation of different types of data
  - Keys
  - Text
  - Data Integrity Codes
  - Personal Identification Numbers
- Some advanced functions associated with cryptography are combinations of basic cryptographic functions applied in a specific manner against specific data

What are the Basic Cryptographic Functions?

- 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.

- Each of the functions have various algorithms one can chose to use AND each algorithm may have parameters that allow the changes to the process of that algorithm

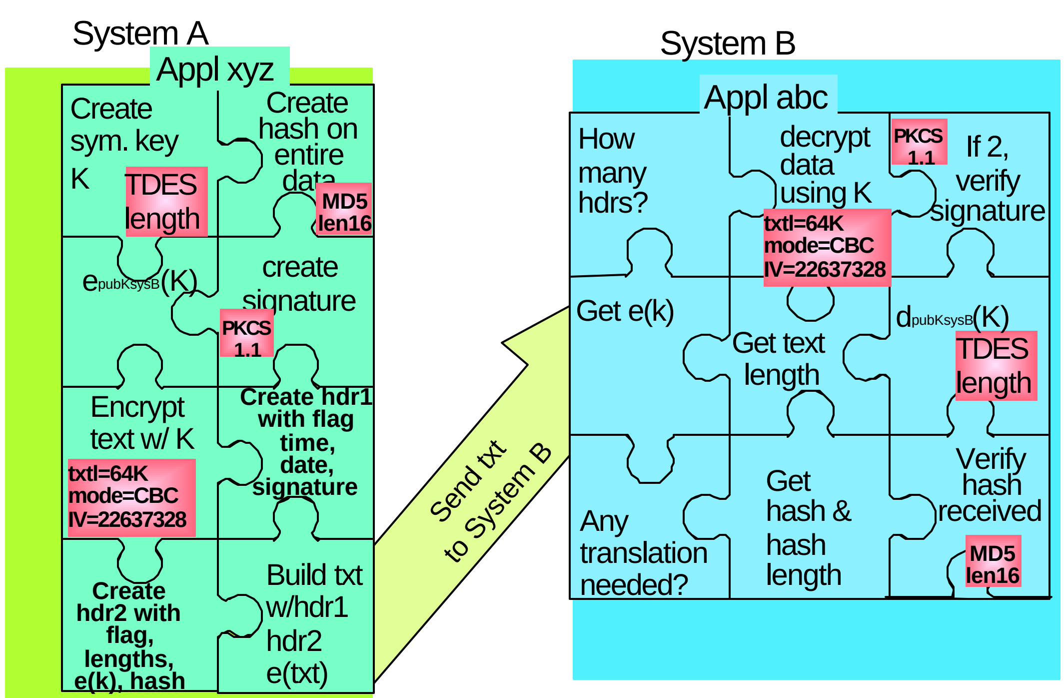
How is Cryptography Used?

- Specified in applications by a user desiring a cryptographic function to be performed
- Specified in protocols and standards based on a common body of participants to create a blueprint that defines the structure of information to be exchanged
  - Using a standard or protocol is like everyone having the same application specification for a specific function
  - Functions written to a specification should work without problems in a heterogeneous environment
- At the core of Cryptography are some basic functions upon which more complex cryptographic structures are built.
- Applications are written to request a cryptographic function, some engine must perform the mathematical processes associated with the algorithms to be used.

Packaging

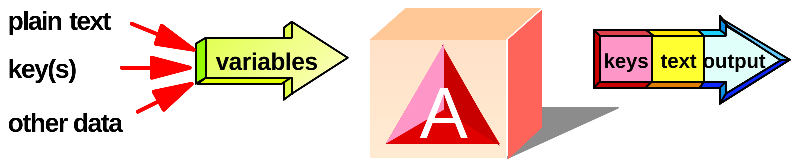
- To be able to know how to reverse an operation that uses cryptography, one needs to know quite a bit about what was done. This info must be communicated somehow.
- To be able to do multiple functions one needs to know even more, for instance, when, how, etc.
- Standards and protocols tell which functions to perform and in what order. This way any application using the standard or protocol will be able to reverse the operation if needed or 'unwrap' the package.
  - Where do I find the key, how is it encrypted?
  - How large is the text, what options where used to encrypt it?
  - Is there a hash on the data? Where is it?
  - On what data is the hash produced, which algorithm, when, ...

Cryptography at Work



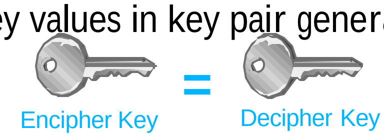
Cryptographic Algorithms

- 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

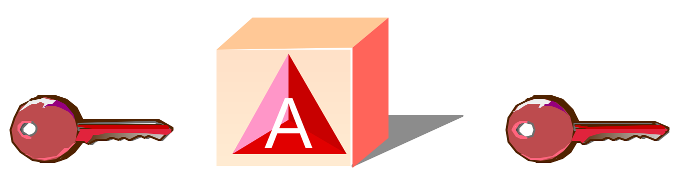


Symmetric Algorithms

- Characterized by identical key values in key pair generation
- Examples:

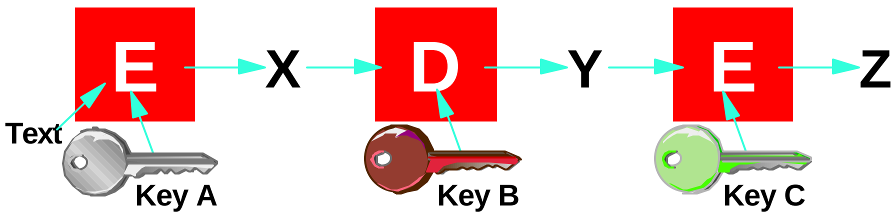


- DEA or DES, Data Encryption Algorithm or Data Encryption Standard
- Triple-DES, DES but using 3 key values rather than 1 key
- CDMF, Commercial Data Masking Facility
- IDEA, International Data Encryption Algorithm
- RC2, Rivest
- RC4

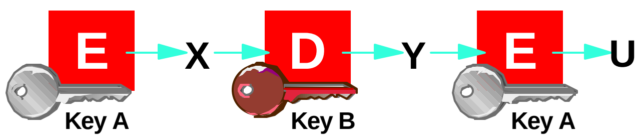


Triple-DES Processing

- TDES is performed with either 3 keys, a true. full-length TDES key or 2 keys.
- Outer Feedback means that when 2 keys are used the first key, Key A, is used again in place of the 3rd key, Key C.
- The processing is

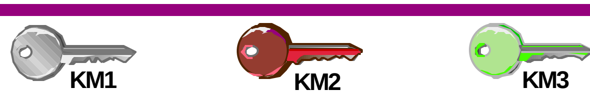


- If only 2 key values are used then processing is



DES Key Length Compatibility

where object (a) & keys



Keys are hexadecimal strings

TRIPLE LENGTH

$e_{KM1}(a)=b$ $d_{KM2}(b)=c$ $e_{KM3}(c)=d$

DOUBLE LENGTH

$e_{KM1}(a)=b$ $d_{KM2}(b)=c$ $e_{KM1}(c)=e$

SINGLE LENGTH

$e_{KM1}(a)=b$ $d_{KM1}(b)=a$ $e_{KM1}(a)=b$

$e_{KM1}(a)=b$ $d_{KM2}(b)=c$ $e_{KM2}(c)=b$

$e_{KM1}(a)=b$ $d_{KM1}(b)=a$ $e_{KM2}(a)=f$

and if KM1 = KM2 then*

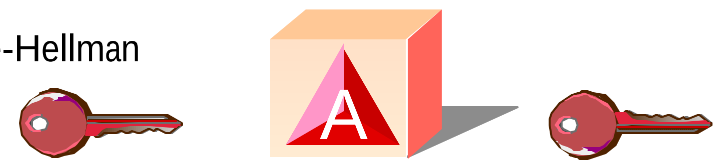
$e_{KM1}(a)=b$ $d_{KM2}(b)=a$ $e_{KM1}(a)=b$

*This part was added to the foil after SecureWorld.

Asymmetric Algorithms

- Characterized by unique key values in key pair generation

- Mathematical computations
  - Using large prime numbers
  - Private key can be used to reverse public key operations
  - Public key can be used to reverse private key operations
- Examples:
- RSA, Rivest Shamir and Adleman
- Diffie-Hellman



Asymmetric Key Use

- 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

- 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

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

Cryptographic Algorithms: A Key Sample

Cryptographic algorithms change the appearance of data

ciphering of a clear key value produces an enciphered key under a master key

Clear Key Values of single-length and double-length DES keys

F3F3F2F1F3F7C4F1   3F3F2F1F3F7C4F1AA22CC7749B9A8F4

Enciphered Values

2BD8DAC0294C78C1   2BD8DAC0294C78C1AA9006F7DBD51E7E

Character Appearance

.Q¹{.<ÌA   .Q¹{.<ÌA¡°.7ûN.=

Cryptographic Algorithms: A Key Sample . . .

In IBM system even clear key values of private asymmetric keys are enciphered under a master key. Here is a private asymmetric key value (read left to right) expressed as the

Secret Exponent, d, the enciphered value

```
1D8DE193C18EA76F3845799A8747D5D9 0BCA793A17317C61254F34AB93A0F350
2E72762AF908C3DF24E216F5893708A8 4C90BAED6C5F66F9D6CDA11A5663151E
F80A10EFE8BB26D5935FC0CB3D449F8E B1486DF95D543B605D8A6E0295B03BC8
CEBCDBAD2E79F2A50EDDC25453A04839 ED00831E3864AC83BC7310F23D774406
```

modulus, n.

```
800000000000000000000000000001D 61D38DC1AFB814FD26E838FD5DBDC7EA
E5328F335AEB2ED667BBC71A2745B13A D0AB62E8887B53DE3A57D4ECB5AEDE47
56C05E83108CCCE213DCFB7EE86F240F A2A6A85D21D9A353C0A733D9C2392578
D09C76AE55682C98BF2E8B97B5B84D7B 278DD9F5B31DA63854478D4B6E654CFB
```

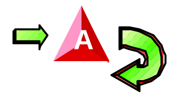
Cryptographic Algorithms: A DES Cipher Sample

Cryptographic algorithms change the appearance of data based on operational selections for the algorithm

DES ciphering of clear text value

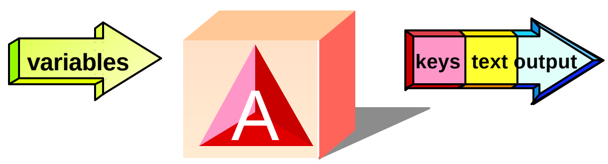
CRYPTO - INTERESTING WORK, GOOD EXERCISE FOR THE MIND BUT ...

using input variables of CBC, IV of all 0's
and one of the key values shown previously
produces ciphertext that looks like



J*.9û!.tÔ¬..Þw^÷Ü©%..'³Ì®¢Ï@Bn-.#4µâ¥.ñ]ÐhÄ-±»?äv.ÌØd¡ÂJ

D15C02F9DB5A0AA3EB5F2313AEA6B0E1 FCB46C05167DFA78AF4A777CC295CA0F
7BF4A042B20149BBAC8863608F8B6F43 A509788084AA62D1D6774BED03E92562



Cryptographic Algorithms: A DES Cipher Sample . . .

Communicating parties must use the same options because use of different options causes different results.

J*.9û!.tÔ¬..Þw^÷Ü©%..'³Ì®¢Ï@Bn-.#4µâ¥.ñ]ÐhÄ-±»?äv.ÌØd¡ÂJ

A encipher of the text using different values for variables
shows the following results in character and hex when using a

- different IV

.%ìÚ.¯ßÔ è|.¸8.c..éP° Ð.ÏF.².Ð!É.».ÀWlÚ!»Áü.Naù./.÷HñÓMh

226C58FE3CBC59EB41544F089DF83783 373451D79040AC1C77C604EA12AC5A71
318B0D64E693FE5A8B65DCFFD581DD13 6111E1C849EED48807368E500F42766D

- different key length (different key)

i¾kTì_³é.w{..XjF..'ßvÇØd¬Á.]ò./gôEç.Y.@CAã.$õ§½.v#.c.û.a

89B992E3586DFA511FA6C01B3BE791C6 1C137D59A56880845F6504BBCD3C6187
CBC54828E8107CC3C1462A5BCFB5B820 A57B258302DB1881BB35FCC821038461

Cryptographic Algorithms: A DES Cipher Sample . . .

A decipher of the enciphered text using different values will not produce the same clear text

- different text length

```
text length too short  ==>  CRYPTO - INTERESTING WORK, GOOD
text length too long   ==>
CRYPTO - INTERESTING WORK, GOOD EXERCISE FOR THE MIND BUT ...
```

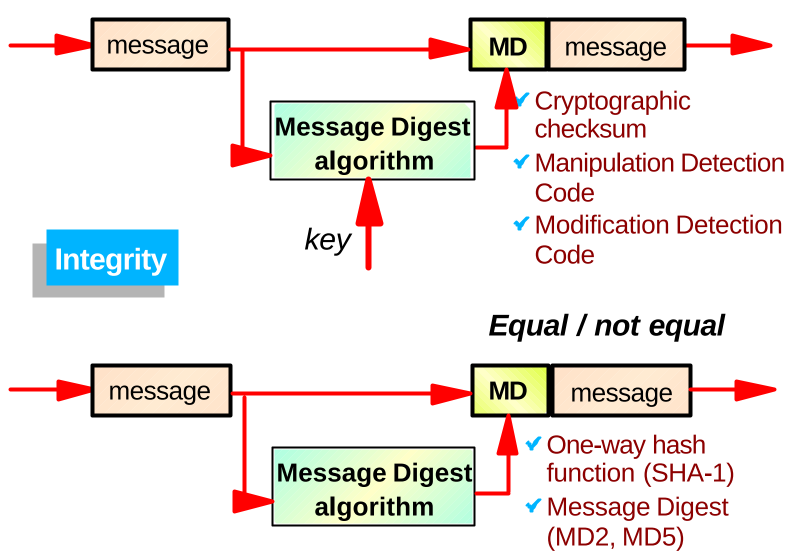
- different IV

```
......ns INTERESTING WORK, GOOD EXERCISE FOR THE MIND BUT ...
```

- different key length (different key)

```
EJìlÈÿ.¿²,.D²'Äñ)¶kvà`T.]¥I.&øçÔ.Wê._Ñ.ùb.¤.¶...ÒJx¬<k.Û).è©ôTýª
```

What Are Message Digests or Hashes?



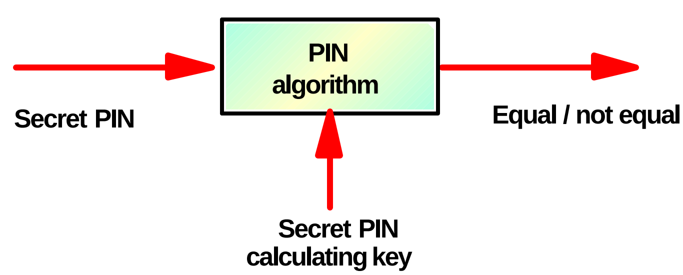
Digests and Hashes: A DES Cipher Sample . . .

The terms message authentication, modification detection, and hash all refer to a process of condensing text using an algorithm to small number of bytes based on the algorithm.

Using the text from earlier, various codes can be produced.

Digest or Hash type	process	text length bytes	CODE
MAC	X9.19OPT	64	0B825524
	X9.19OPT		0B825524C74B72E4
	X9.19OPT	32	C591DB8B
MDC	MDC-2	64	5712128D9E7F4D915FE5784B19BFAC8E
	MDC-4		72DB176E3873FFB04D0DCE877A450527
One Way Hash	SHA-1	64	81F3BBC69C85D462F2B59E62457660F08A194D51
	MD5	64	B29A7065A8536B471790CCBE98AD54E3

What Else? PINs



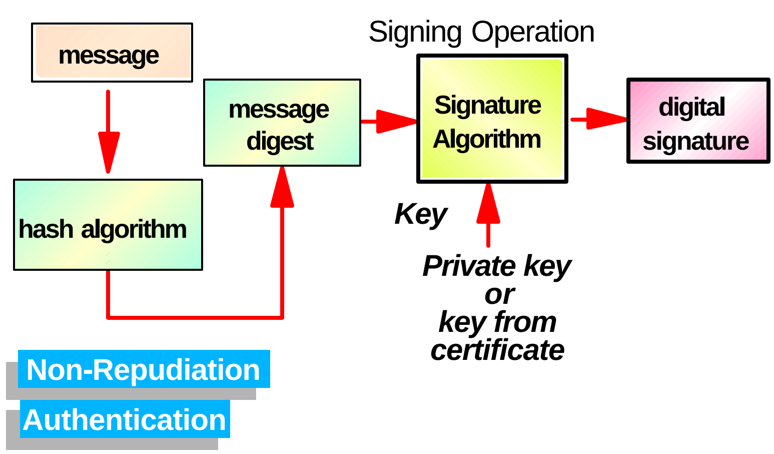
Authentication

PINs

- Personal Identification Numbers have long been used. There are algorithms for producing a PIN in a format that makes it difficult to determine the PIN value used. Formats are necessary since PIN values are usually only 4 or 6 digits.
- Algorithms
  - 3624
  - German Banking
  - PIN Offset
  - PVV
  - Interbank

What Are Signatures?

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



Signature Samples

Using the text from earlier and the SHA-1 and MD5 hashes of that text, here are the IS0-9796 digital signatures created.

- SHA-1 of 81F3BBC69C85D462F2B59E62457660F08A194D51
- Produces

.tØÓ\.R¿....Ð..ø.ÀãG}ÅZDr»yþ¯/y<0/)4Ò)..Uvâ.j$C§]d.!¼¢U.½v.ÅG...
éò.¯³'§gg .t...+£z.ì.)Hß3.ï..^ïÍöz]¬ÿ.QÑp÷3.ßÚZ.Ö³.6¿.{ú`ÌVq,³=!

- MD5 of B29A7065A8536B471790CCBE98AD54E3
- Produces

.a¡æsvÌ3...\Ð..Z.éë.Ù¬?r'Z"å.Ü.».³º.L.´íK).Ãëùþ.CS..\..UÓpa.ëÅ.¦
Î.¥Ö¦.Íë..Ôòü.ð%w®.!¢Ãá.¨ý%´ýfî¶½ýD².å?N.FÃ.¢nMEo¹Ä°../@..&ª/.Îü

Signature Samples . . .

Using the text from earlier and the SHA-1 and MD5 hashes of that text, here are the digital signatures created using ZERO-PAD.

- SHA-1 of 81F3BBC69C85D462F2B59E62457660F08A194D51
- Produces

...ídÉ°à=.Ëy.º.^o..lPq¢j®°Ú.»Ð9..5JäÖÒí>.\.x4Éâ¼¿.c'ÒÐ¸ñðP®çg§..
.fç».C.Rè.b¼JaË,ä{¢7.?.¡zõDä.Ü.1..×fò..Àh..èw.._..LK¨Ð.c*¨º bwEû

- MD5 of B29A7065A8536B471790CCBE98AD54E3
- Produces

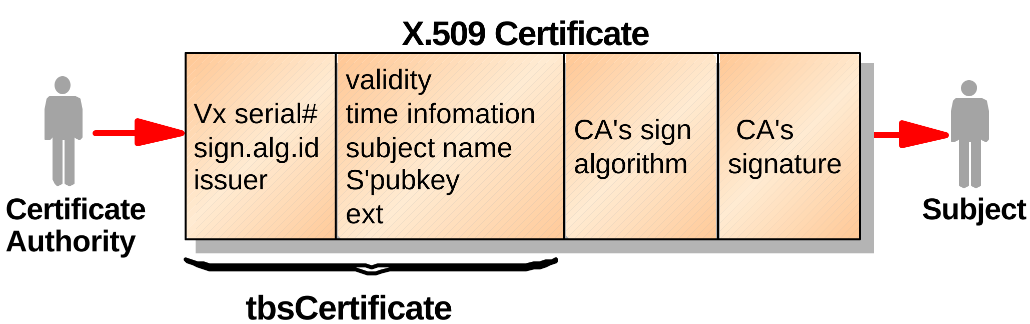
.§9Oã.jZØ.wPÄoH#ð_rê..±Ïv.5N2¸/i%bö÷ytú...âb¯AnÏÃÍ.Ç.. ö.¼ü¢./ç.
I.s.Ú.è.'ÏÓB..LXòyÍ4&+mþ.âh..ñ...ã*.ç}HàQ.¼.\.à..5..¢Ø.oFÀÛ.².ÿè

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
  - eprivate 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 DER encoding is a tag, length, value encoding system for each element.

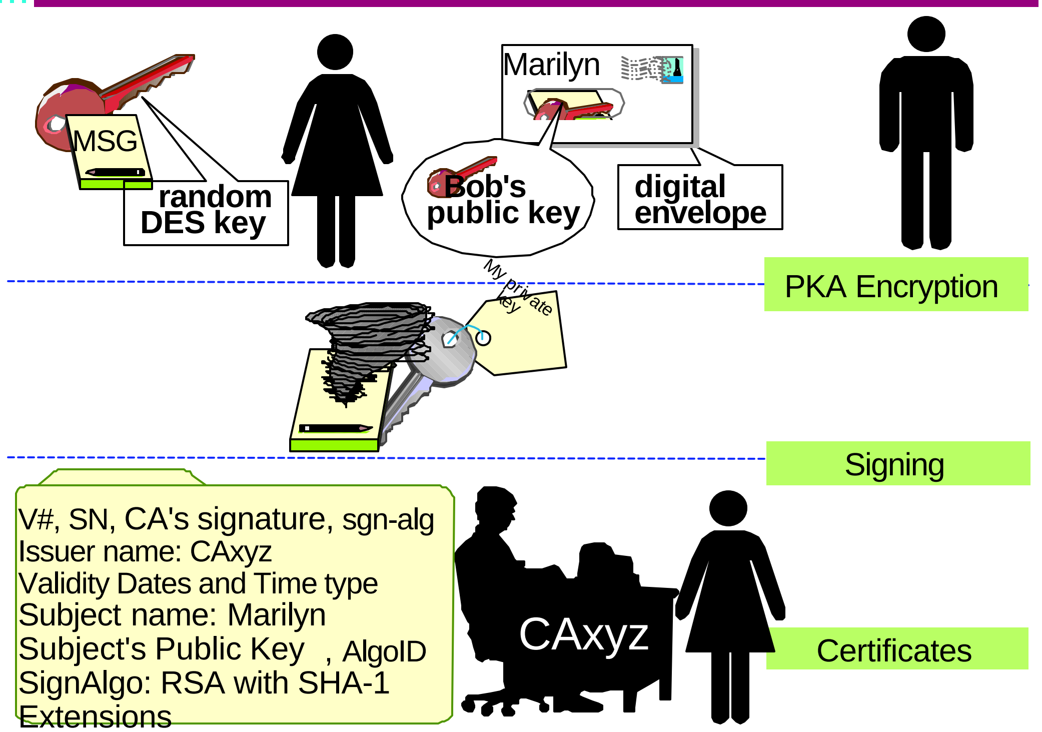


Authentication

Certificates . . .

- Subject's Name
  - X.501 type Name
- Subject's Public Key
  - carry the public key of the subject and
  - identify the signature algorithm with which the public key is used
  - SEQUENCE
    - algorithm referred to as the OBJECT IDENTIFIER,
    - parameters referred to by ANY DEFINED BY algorithm and are optional
  - where the algorithm is rsaEncryption, the structure contains a modulus, n and a public Exponent, e

Complex Ideas: Signatures and Certificates



Going From Here to There

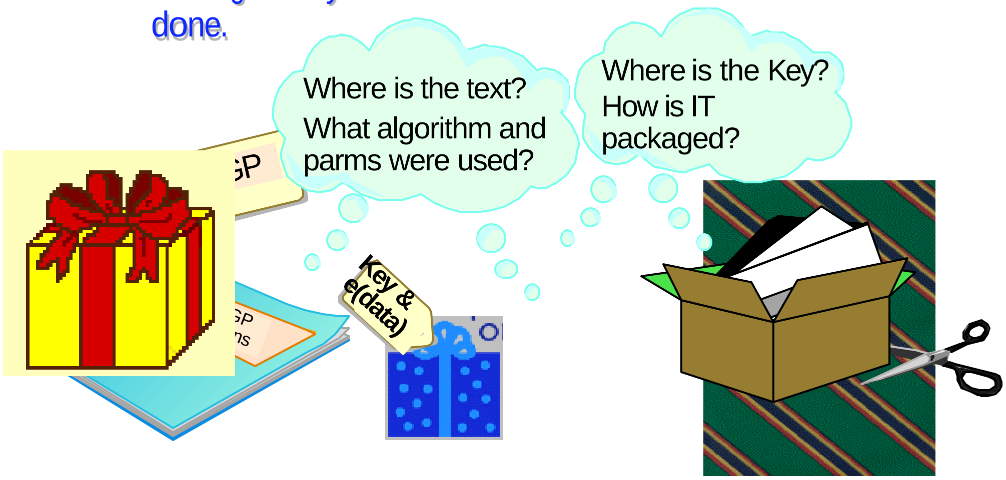
- Same type algorithm? Same processing method?
  - DES => DES? yes
  - DES => IDEA? no
  - RSA => RSA? yes
  - RSA => Elliptic Curve? no
- Same key association? Same length capability?
  - DES key value (a) = DES key value (a+n)? no
  - DES key value (a) = DES key value (a)? yes
  - RSA key value ($b_{len1024}$) = RSA key value (b_{len512})? no
  - RSA key value ($b_{len1024}$) = RSA key value ($b_{len1024}$)? yes
  - RSA key ($e_{\text{joe's public key}}$(msg)) => RSA key ($d_{\text{bob's private key}}$(msg)) no

Going From Here to There . . .

- Applications vs Enablers
  - Some products provide a mechanism for doing cryptographic functions with some configuration or no external requirements.
  - These products are applications which use cryptographic functions in a predetermined manner.
- PGP - Pretty Good Privacy
  - Provides specific function based on GUI selection
  - Application code manages the creation of the "packaged" text and key infomation
- BSAFE, ICSF
  - Provide coding mechanisms for application selection of function
  - User written code must use those Application Programming Interfaces to create their desired "packaging"

Going From Here to There . . .

- In English....
  - Unless you want to write your own application to conform to an application's "package", you must always use the application at both ends of the transmission.
  - Packages may not be well documented as to all that must be done.



Summary

- Most cryptographic functions have selections of parameters that can be specified to change the outcome of the algorithm.
  - key length
  - type of processing based on some standard
  - whether a specific input value was provided for an option
  - text length
  - etc.
- For the complex requests and application functions, packaging issues become part of the things on which your request may be dependent.
- These are the "gotchas" in most situations where data and/or keys are exchanged. Most can be bypassed by using standards and understanding how those standards affect the cryptographic function.

References

- Bruce Schneier, "Applied Cryptography Second Edition : protocols, algorithms, and source code in C", John Wiley & Sons, Inc., 1996
- Richard E. Smith, "Internet Cryptography", Addison-Wesley Longman, Inc., 1997
- Vijay Ahuja, "Network & Internet Security", Academic Press, Inc., 1996
- Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security PRIVATE Communication in a PUBLIC World", Prentice Hall, Inc., 1995

The End