IBM

zSTSU 2004
Crypto Concepts From A Business View

Greg Boyd
December 7, 2004
IBM Washington Systems Center
Advanced Technical Support
Gaithersburg, MD
boydgy@us.ibm.com

1

IBM

Data Confidentiality

- ***Symmetric Key***
  - ***–DES/TDES***
  - – AES
- Asymmetric Key
  - – RSA

2

IBM

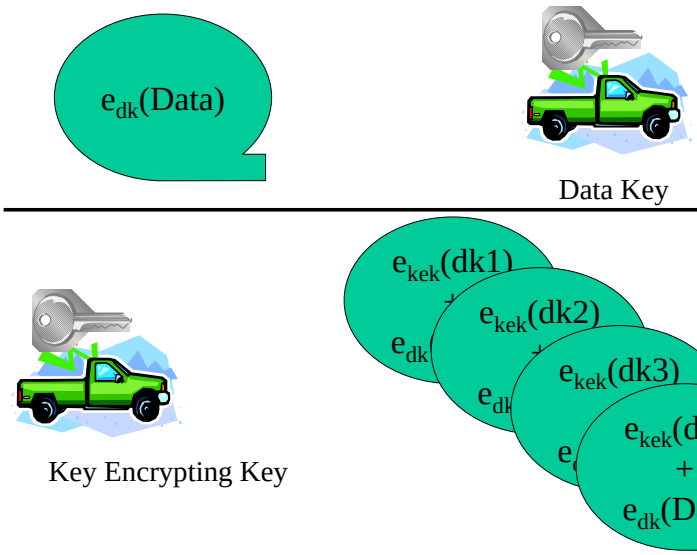
Data Confidentiality

- ***Symmetric Key***
  - DES/TDES
  - ***AES***
- Asymmetric Key
  - RSA

3

IBM

Symmetric Key



4

IBM

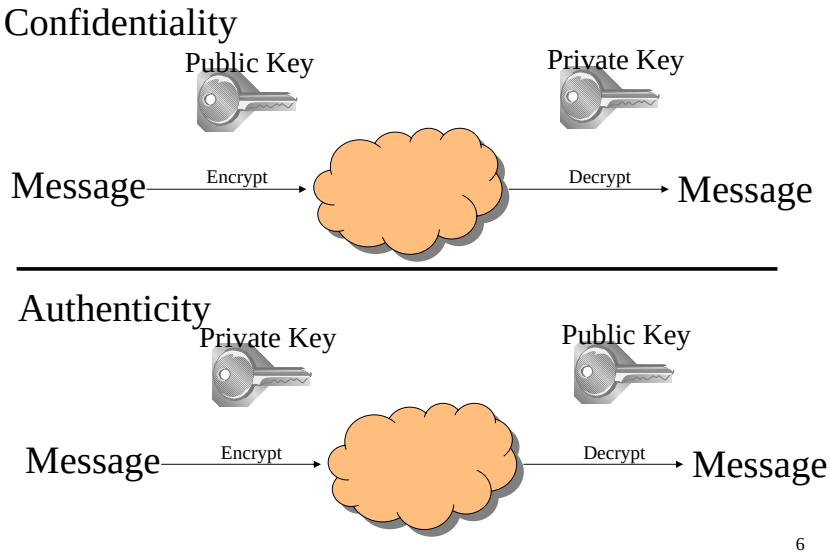
Data Confidentiality

- Symmetric Key
  - DES/TDES
  - AES
- ***Asymmetric Key***
  - ***RSA***

5

IBM

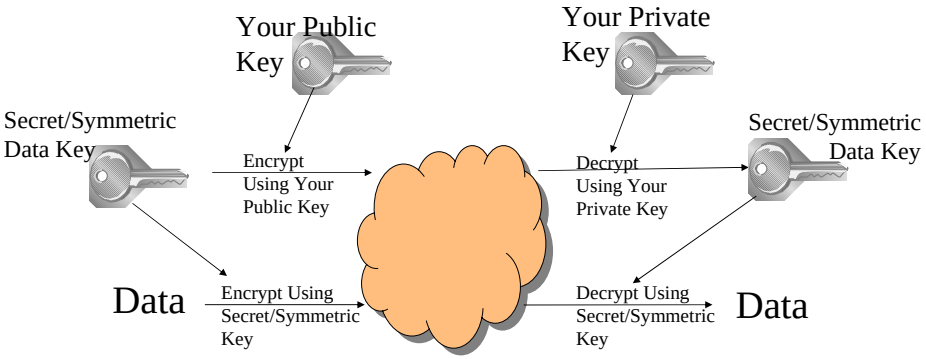
Public Key Architecture



6

IBM

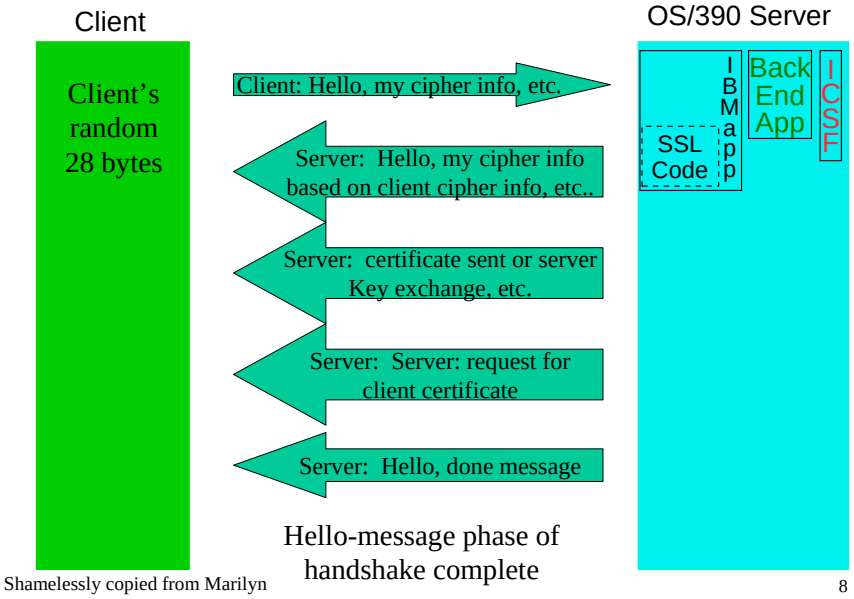
Combining PKA & Symmetric Key



7

IBM

SSL Handshake: Hello

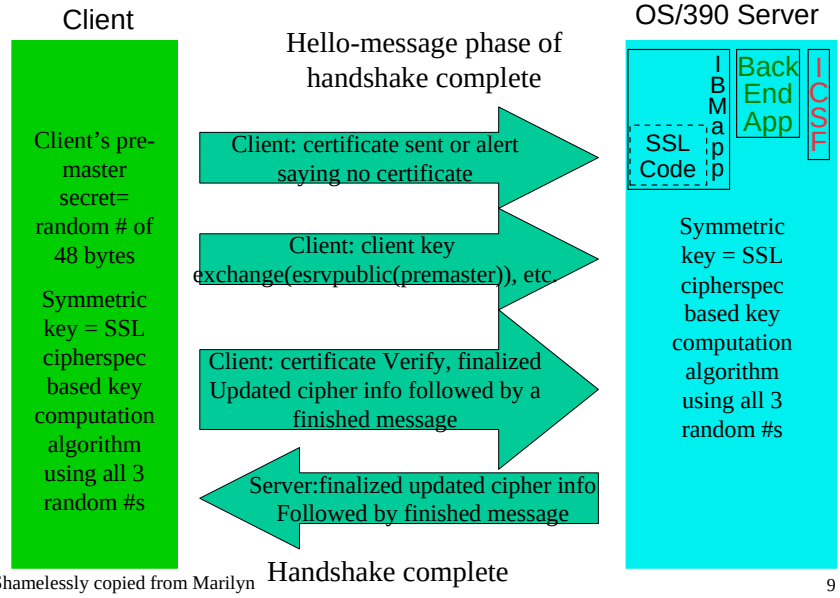


Shamelessly copied from Marilyn Allmond's ES801 class foils

8

IBM

SSL Handshake: Hello



Shamelessly copied from Marilyn Allmond's ES801 class foils

9

IBM

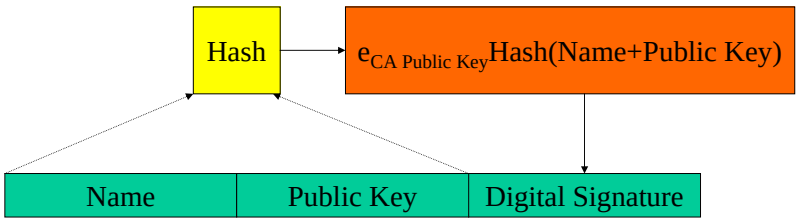
Data Integrity

- ***Hashing***
- ***Message Authentication***
- ***Modificaton Detection***

10

IBM

Digital Certificates



11

IBM

Financial Functions

- ***PIN Generate (Clear & Encrypted)***
- ***PIN Verify***
- ***PIN Translate***
- ***Secure Electronic Transaction (SET)***

12

IBM

Key Management

- *Master Keys*
- *Key-Encrypting-Keys*
- *Data Keys*

- *CKDS - Cryptographic Key Data Set*
- *PKDS - PKA Key Data Set*
- *ICSF Data Space/Hardware Registers*

13

IBM

Utility Functions

- *Random Number Generation*
- *Code Conversion*
- *Character/Nibble Conversion*

14

IBM

Legislation

- **California SB 1386**
- **Gramm-Leach Bliley Act**
- **Sarbanes-Oxley (SOX)**

15

IBM

California SB1386

- Effective July 1, 2003
- Business in CA or businesses w/customers in CA
- Demonstrate due diligence in protecting customer data
- Disclose first name or initial and last name and data like SSN, or drivers license number, and not encrypted
- Must expediently notify that individual of any security breach, unless the data is encrypted

16

IBM

Financial Modernization Act Gramm-Leach Bliley

- Applies to Financial Institutions
- Privacy Notice
- Prohibited from disclosing customer account numbers to non-affiliated companies for telemarketing, direct mail marketing or other marketing through e-mail – even if the individuals have not oped out

17

IBM

Sarbanes-Oxley

- Corporate Governance
- Financial Reporting
- Executive Conduct
- Internal Controls
  - Certification of disclosure controls

18

IBM

z890/z990 Features

- CPACF

- 0862 PCICA
- 0863 Crypto Express2*
- 0868 PCIXCC*

*Denotes Secure Key

19

IBM

z800/z900 Features

- 0800 CCF*
- 0861 PCICC*
- 0862 PCICA

*Denotes Secure Key

20

IBM

G6 Features

- 0800 CCF*
- 0860 PCI Cryptographic Coprocessor*

*Denotes Secure Key

21

IBM

Internal References

- ATS TechDocs – http://www.ibm.com/support/techdocs (then Choose Search All Documents, use keyword Crypto)
- Pubs
  - SA22-7519 ICSF Overview
  - SA22-7521 ICSF Administrator's Guide
  - SG24-6870 zSeries Crypto Guide Update

22

IBM

External References

- Cryptography Books
  - 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
  - Niels Ferguson, Bruce Schneier, "Practical Cryptography", Wiley Publishing, Inc., 2003
- Free Stuff
  - http://infosecuritymag.techtarget.com
  - http://www.scmagazine.com/home/index.cfm
  - http://www.counterpane.com

23