INTRODUCTION
to
CRYPTOGRAPHY
&
CRYPTOGRAPHIC SERVICES
on
Z/OS

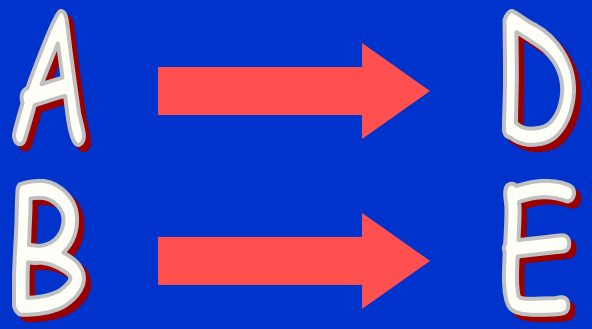
BOSTON UNIVERSITY SECURITY CAMP

MARCH 14, 2003

History of Cryptography

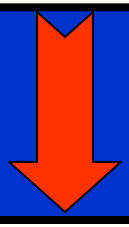
- The concept of securing messages through cryptography has a long history.
- Julius Caesar is credited with creating one of the earliest cryptographic systems to send military messages to his generals.

CAESAR'S SHIFT BY 3 RULE

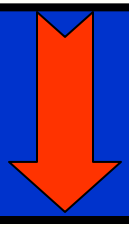


What Is Cryptography?

As the field of cryptography has advanced, the dividing lines for what is and what is not cryptography have become blurred.

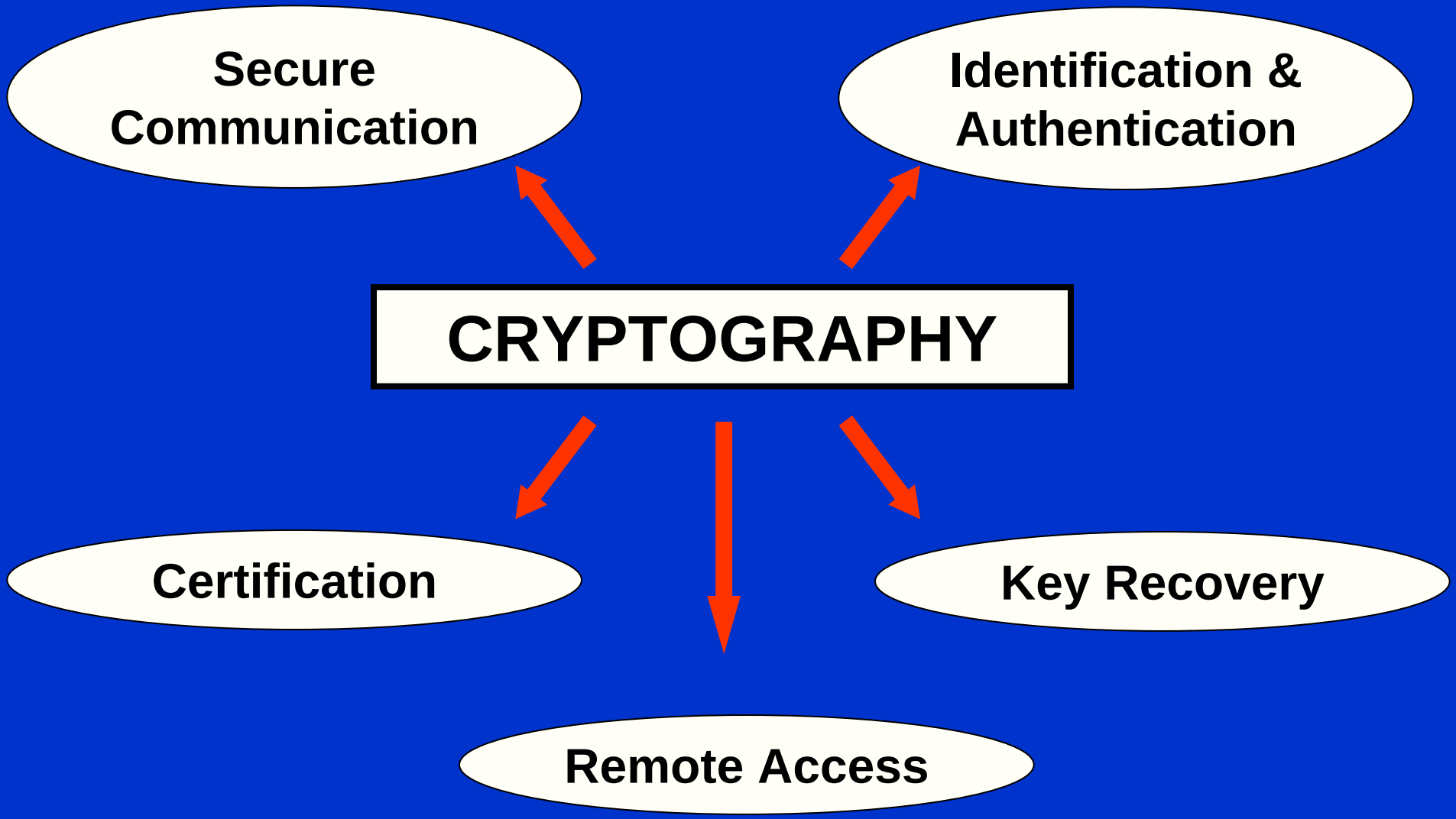


Cryptography today might be summed up as the study of techniques and applications that depend on the existence of difficult problems.



But the field of cryptography contains even more when we include some of the things cryptography enables us to do

How is it Applied?



How Does Cryptography Work?

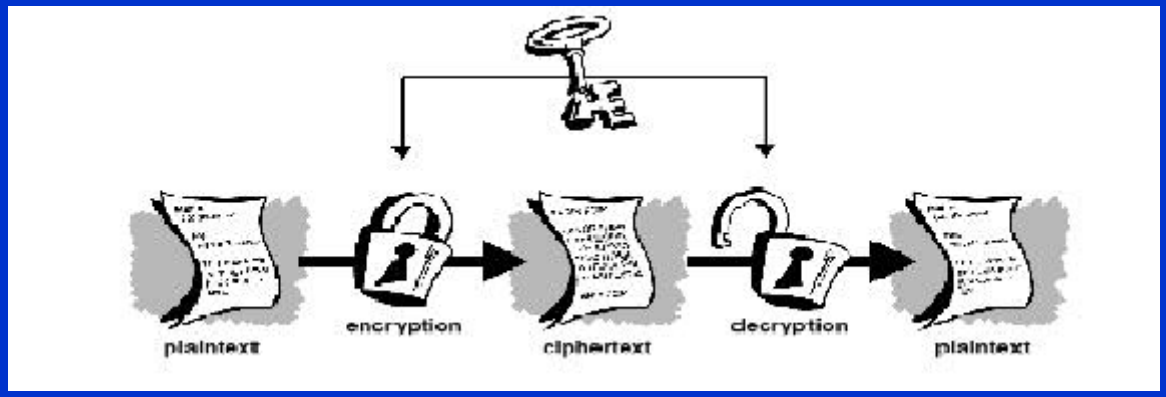
- A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process.
- A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext.
- The same plaintext encrypts to different cipher text with different keys.
- The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.
- A cryptographic algorithm, plus all possible keys and all the protocols that make it work, comprise a cryptosystem.

Basic Elements of Cryptography

- **Encryption:** converts data into some unreadable form
- **Decryption:** transforms the encrypted data back into its original, intelligible form and serves as the reverse of encryption
- **Authentication:** can be used to identify (individual user, a machine, an organization, etc)
- **Digital signatures:** serves as the digital equivalent of paper signatures by binding a document to the holder of a particular key
- **Signature verification:** verifies the validity of a particular signature

Symmetric Key Encryption

- In symmetric-key encryption, one key is used both for encryption and decryption.



PRO

Very efficient use of CPU for bulk data

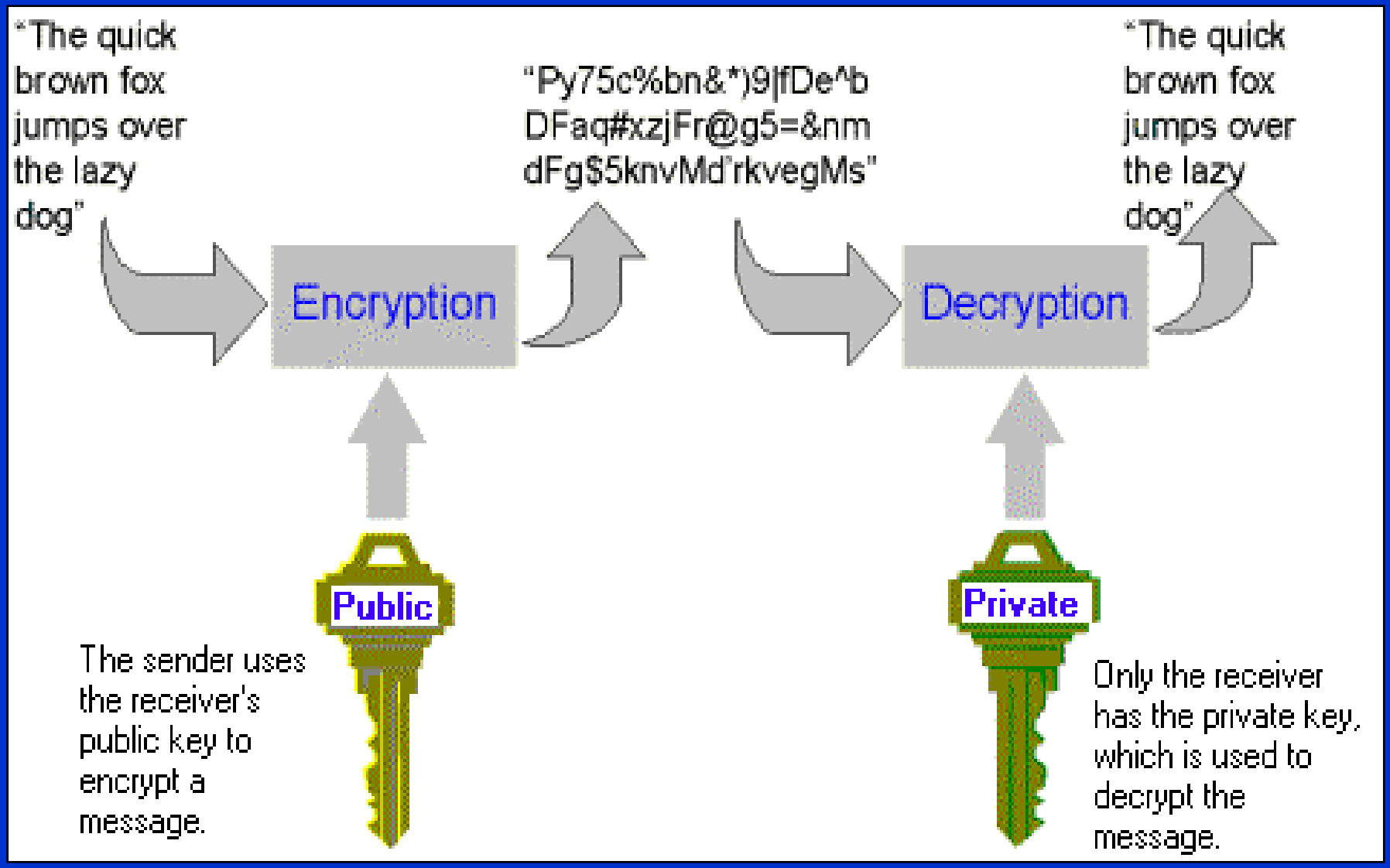
CON

Key Management and Security Issues (Large number of business partners; keys decrypting data can exist in more than one place)

Public-Key Cryptography

- Removes the need to use the same key for encryption and decryption
- Key Pairs are Used (Public/Private)
  - Public Key: Shared with Business Partner's and used to encrypt data
  - Private Key: Kept by the key pair owner and used almost exclusively for decryption. This key is *never* shared
- Not subject to same key management and security issues as symmetric keys
- Matched "public" and "private" keys
- Prior to the invention of public-key cryptography, it was very difficult to provide key management for large-scale networks

Public-Key Encryption: Two Keys



Common Public-Key Algorithms

- **RSA: for both digital signatures and key exchange.** The Rivest-Shamir-Adleman (RSA) cryptographic algorithms are the most widely used public-key algorithms today, especially for data sent over the Internet.
- **DSA: for digital signatures only.** The Digital Signature Algorithm (DSA), invented by the United States National Security Agency (NSA).
- **Diffie-Hellman: for key exchange only.** Diffie-Hellman, the first public-key algorithm invented.

Using Public-Key Encryption for Digital Signatures

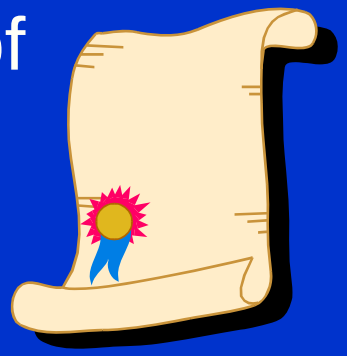
- Is a means for originators of a message, file, etc. to provide a signature for the information.
- Frequently, digital signatures are used when data is distributed in cleartext

Authentication
(Who Is The Data From)

- **Signing Provides Non-Repudiation** *(User Cannot Deny the Data is Theirs)*
- **Sender Encrypts Signature with Private Key**
- **Receiver Decrypts Signature with Public Key**

Certificate

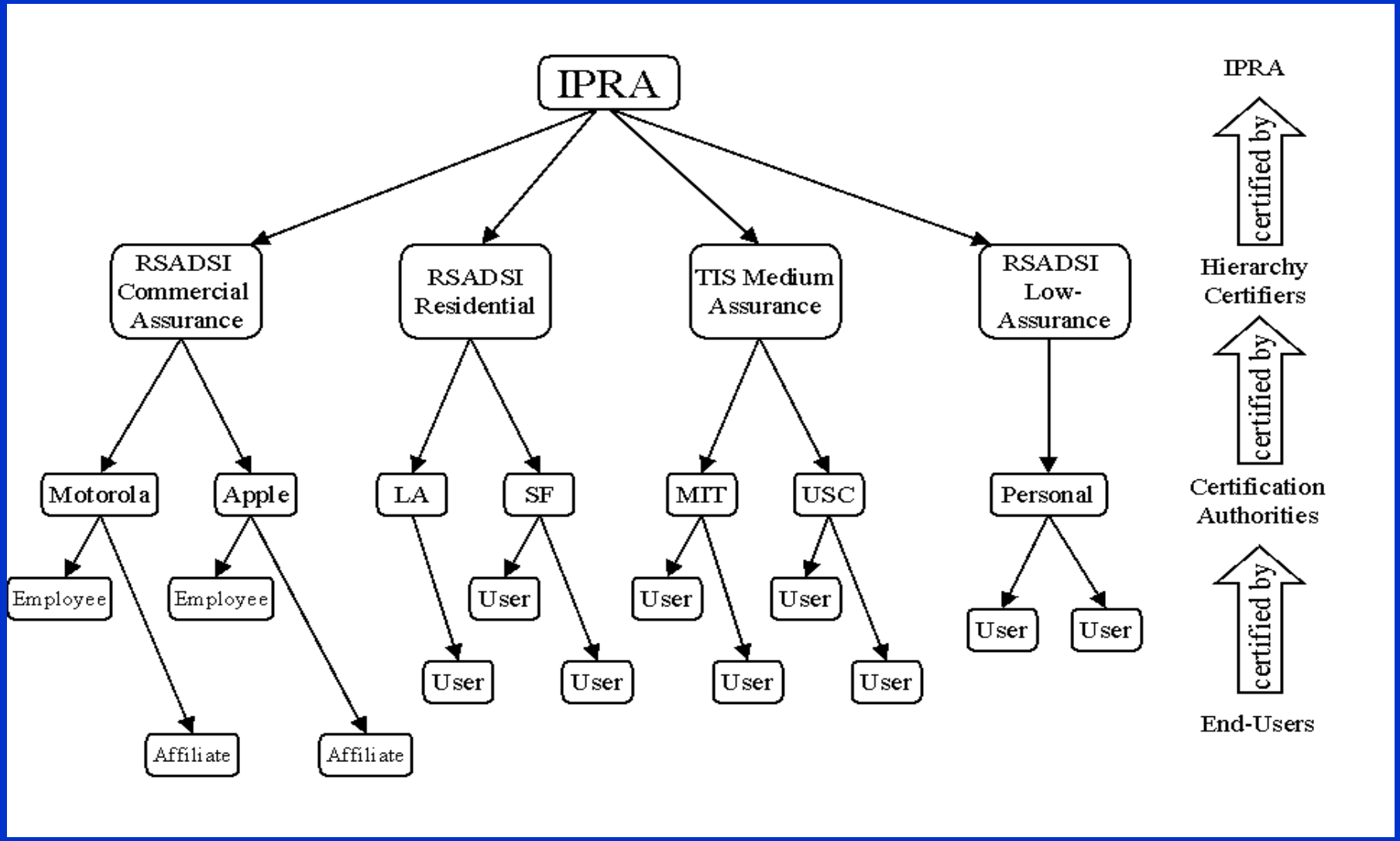
- A ***public key certificate***, often referred to simply as a ***certificate***, is used for authentication and secure exchange of information on the Internet, extranets, and intranets.
- A public key certificate is a digitally signed statement that binds the value of a public key to the identity of the subject *(person, device, or service)* that holds the corresponding private key.
- Certificates can be issued for a variety of functions.



Certification Authority

- A ***certification authority*** (CA) is an entity trusted to issue certificates to an individual, a computer, or any other requesting entity.
- A CA can be a remote third party
- Three Types of CAs
  - Self-Signed CA
  - Subordinate CA
  - Root CA

Example of a Certification Hierarchy



Key Management

- ***Key Management*** deals with the secure generation, distribution, and storage of keys.
- Users must be able to securely obtain a key pair suited to their efficiency and security needs.
- If the private key is lost or compromised, procedures to notify others must be in place to minimize the exposure.

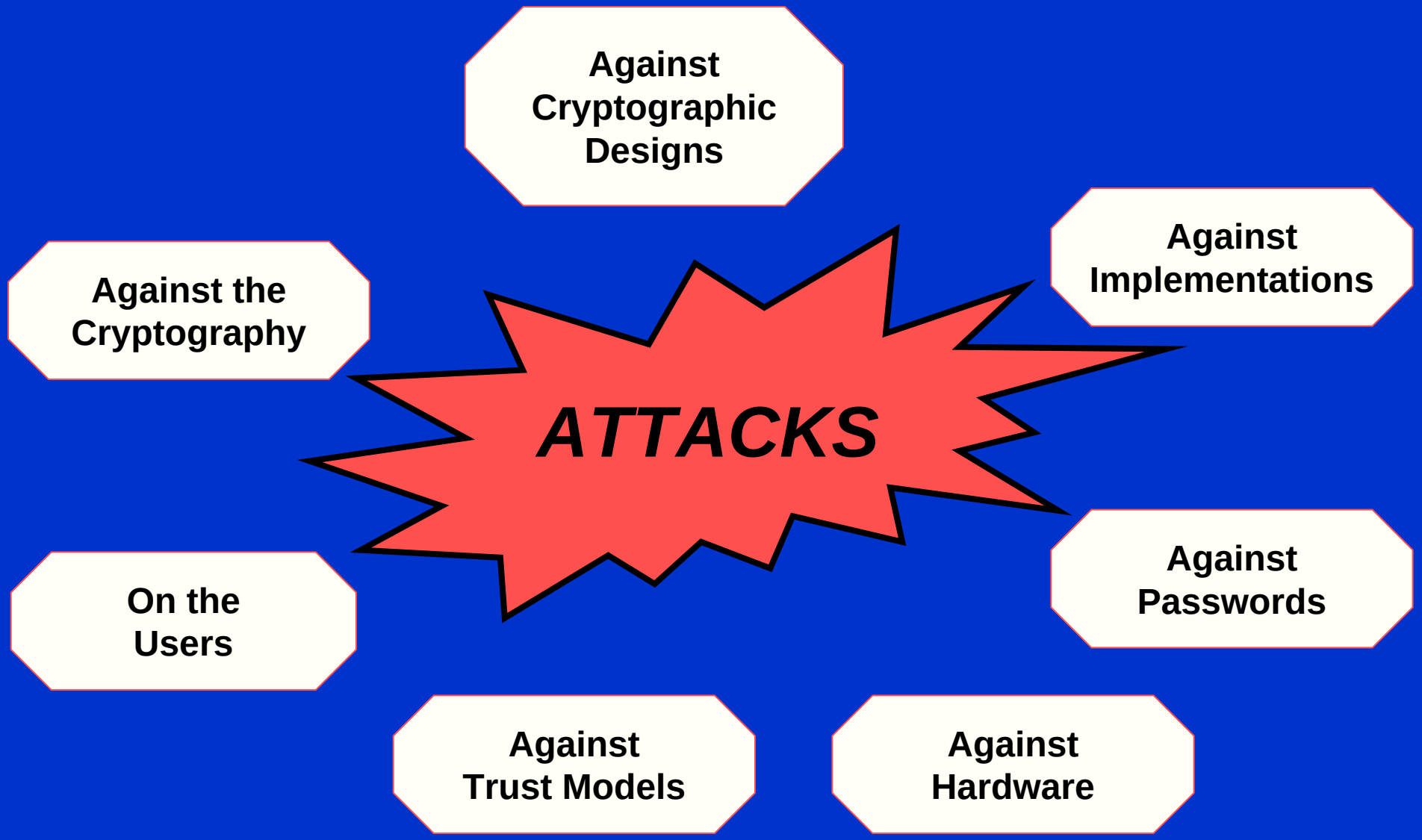
Key Size

- What size key do I need?
- What is the life cycle of a key?

W. Ford, Computer Communications Security Principles, describes the cycle as:

1. Key generation and possibly registration (for a public key)
2. Key distribution
3. Key activation / deactivation
4. Key replacement or key update
5. Key revocation
6. Key termination, involving destruction or possibly archival
7. www.rsasecurity.com/rsalabs/ for current information on recommended key sizes

Security Pitfalls



Overview of the z/OS Cryptographic Coprocessor

- The Cryptographic Coprocessor hardware is implemented in CMOS technology on a single chip providing more capability than any previous cryptographic offering.
- Included in the design is battery-backed non-volatile memory storage, laser delete chip personalization, integrated tamper detection and response, and high speed DES, Triple DES, DSS, RSA, Pseudo Random Number Generation, and hashing algorithms.

Cryptographic Coprocessor

- The Cryptographic Coprocessor Feature includes one or two cryptographic coprocessor chips protected by tamper-detection circuitry and a cryptographic battery unit.

The powerful IBM @server zSeries 800

Cryptographic Coprocessor

- **Dual Cryptographic Coprocessors on Dyadics and above:** Each Cryptographic Coprocessor attaches to two Central Processors to help maximize availability for CP failure events.
- **SET Support:** Secure Electronic Transaction (SET) is a protocol developed jointly by VISA International and MasterCard to help safeguard payment card purchases made over open networks.
- **PKA Cryptographic Key Data Set:** ICSF now provides a storage data set for Public Key Algorithm (PKA) private and public keys.

Cryptographic Coprocessor

- **Support for CVV and CVC:** VISA and MasterCard have specified a cryptographic method of calculating a value that relates to information on a payment card, such as the personal account number (PAN), the card expiration date, and the service code
- **Double-Key MAC Support:** The ANSI X9.19 MAC Procedure is supported by ICSF. This requires the use of a double-length key for MAC processing
- **Triple DES (TDES):** DES encryption for ICSF has been enhanced to now include TDES (168 bits) encryption
- **Awarded** the U.S. government's highest certification for commercial security

Integrated Cryptographic Service Facility Overview

- ICSF works with the hardware cryptographic feature and the Z/OS Security Server to provide secure high-speed cryptographic services in the Z/OS environment.
- The Integrated Cryptographic Service Facility provides the application programming interfaces by which applications request the cryptographic services to the cryptographic feature. The cryptographic feature is a secure high-speed hardware that performs the actual cryptographic functions.
- ICSF runs as a started task and has its own address space and a data space.
- Balanced, expandable support for secure Web serving.
- Greatly improves SSL transaction throughput making secure, high performance e-business applications easier to implement

ICSF Provides Services For:

- Entering keys into both the tamper-resistant hardware and the cryptographic key data set (CKDS and PKDS). Even the final steps of Master Key entry from TKE are performed through ICSF
- Managing and creating cryptographic keys for application use
- For public key cryptography, Z/OS ICSF supports both the RSA algorithm and the NIST Digital Signature Standard

Application Program Interfaces

- Full DES with PKA
- DES with exportable PKA
- CDMF with exportable PKA
- Supporting the ANSI X9.17 key management standard
- Distributing DATA keys enciphered under a RSA key
- Generating and verifying digital signatures
- Composing and decomposing SET blocks

Algorithms Supported on Z/OS

- **Encryption / Decryption**
  - **DES *(Data Encryption Standard)***
    - **Symmetric, 64 block cipher**
    - **56 bit key size**
  - **Triple DES**
    - **“DES times 3” with three different keys (K1, K2, K3)**
    - **Equivalent to 168 bit key size**

More Algorithms on Z/OS

- **Encryption / Decryption**
  - **AES (Advanced Encryption Standard)**
    - **Symmetric**
    - **Supports 128, 192 and 256 bit key sizes**
    - **Blowfish**
    - **Symmetric block cipher**
    - **Variable length key from 32-448 bits**
    - **Standard (16 round) and Fast (10 round) Modes**

More Algorithms on Z/OS

- **Encryption / Decryption**
  - **For all Symmetric Algorithms, the Following Modes are Supported:**
    - **ECB (Electronic Codebook)**
    - **CBC (Cipher Block Chaining)**
    - **CFB (Cipher Feedback)**

More Algorithms on Z/OS

- **Encryption / Decryption**
  - **Cast**
    - **DES-like (16 round)**
    - **Used extensively by PGP and GnuPG**
  - **Diffie-Hellman Elgamal**
    - **Used for public key encryption**
  - **RSA**
    - **uses *modular & exponential arithmetic***
    - **Used for public key and digital signature encryption**

More Algorithms on Z/OS

- **Digital Signature**
  - DSA (Digital Signature Algorithm)
  - RSA (Rivest/Shamir/Adelman algorithm)
  - Secure Sockets Layer – Available as a port to the Unix Systems Services side of Z/OS.
  - Secure Shell – Available as a port to the Unix Systems Services side of Z/OS.
  - Kerberos – has been available since earlier release of OS/390.

Some New Technology

- ***Quantum Cryptography*** is a method for secure key exchange over an insecure channel based on the nature of *photons*.
- ***DNA Computing***, also known as *molecular computing*, is a new approach to massively parallel computation based on ground-breaking work by Adleman.
- **Biometric Techniques** applies to a broad range of electronic techniques that employ the physical characteristics of human beings as a means of authentication.

Evaluating Cryptograph Software

- Which information needs to be protected?
- How well does it need to be protected?
- Is encryption of the data better than other possibilities?
- Who will maintain the encryption keys and be responsible for performing the encryption and decryption?
- Who might attempt to gain access to the information, and what level of cryptanalytic skills might they possess?
- What methods of encryption are available, how much do they cost and what are their merits?
- Should different methods of encryption be used for different kinds of information?
- Is the software compatible with the hardware and the operating system that it is to be used on?

Reference hermetic.nofadz.com/crypto/eval.htm for these and other Observations.

Don’t Roll the Dice on Security

References

- WWW.ASPG.COM – Megacryption Vendor
- WWW.INTERNET.ABOUT.COM/ Cryptography and PKI Basics
- WWW.IBM.COM – Cryptography Essentials
- WWW.INTERNET.ABOUT.COM – What is Cryptography
- WWW.IACR.ORG – Cryptologic Research
- Cryptography for the Internet – Philip Zimmermann Scientific America
- WWW.CRYPTO.ORG Internet Privacy Coalition
- Technology and Privacy – Philip Agre and Marc Rotenberg, MIT Press 1997
- W. Ford, Computer Communications Security Principles,
- *Standard Protocols and Techniques*, Prentice-Hall, New Jersey (1994).
- www.rsasecurity.com
- www.ssh.fi
- K.E.B. Hickman, The SSL Protocol
- www.netscape.com
- www.microsoft.com
- www.nai.com

References

- Aho, Hopcroft and Ullman, The Design and Analysis of Computer Algorithms
- American National Standards Institute, ANSI X9.9 Financial Institution Message Authentication
- Applied Cryptography (2nd Ed.) by Bruce Schneier
- Computer Generated Random Numbers by David W. Deley
- www.counterpane.com/whycrypto.html
- Why Cryptography is Harder Than It Looks by Bruce Schneier
- crypto.cs.mcgill.ca/
- www.gocsi.com/
- www.privacy.org/
- securitytracker.com/
- www.verisign.com/
- www.linuxsavvy.com/staff/jgotts/underground.html
- www.acm.org
- www.iee.org

USA