CITICORP INFORMATION SECURITY OFFICE

Data Classification, Controls & Encryption

Stephen R. Katz
Chief Information Security Officer
Citibank N.A.

Agenda

- Establishing a Common Vocabulary
- Citicorp’s Information Classification
- Control Requirements
- Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography

Establishing a Common Vocabulary

- Do we know who is using the service?
- Can we control what they do?
- Can we ensure the privacy of information?
- Can we prevent unauthorized changes to information?
- Can we provide for non-repudiation of a transaction?
- Do we know
  - if there is a problem?
  - soon enough to take appropriate action?
  - how to minimize / contain the problem?
- Can we prevent denial of service?

Citicorp’s Information Classification Control Requirements

- Restricted
  - Strategic planning information or information on mergers, acquisitions or financial forecasts/results or Passwords or PINs.
- Confidential
  - Information that can be shared on a need to know basis; e.g. product or system development information, marketing strategies, audit reports, information providing competitive advantage.

Citicorp's Information Classification Control Requriements

- Internal
  - Information that can be freely shared among staff. A non-disclosure agreement is required for consultants, vendors, and temps; e.g. operating procedures, policies, interoffice memos, internal phone directories.
- Public
  - Information that is intended for public use by the information owner.

Citicorp's Information Classification Control Requirements

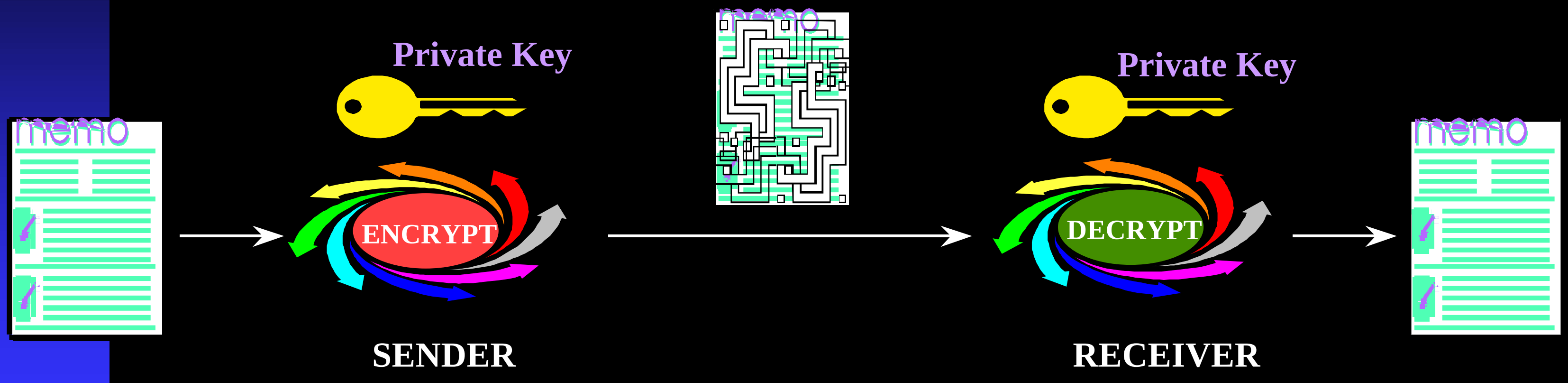
	Restricted	Confidential	Internal	Public
Encryption	**Transit & Storage**	**Transit**	**Optional**	**NA**
Integrity	**Transit**	**Transit**	**Optional**	**NA**
Non-Repudiation	**Transit for financial & changes to demographic transactions**	**Transit for financial & changes to demographic transactions**	**Optional**	**NA**
Disposal	**Permanent Destruction**	**Permanent Destruction**	**Permanent Destruction**	**NA**

Cryptography - The Science of Translating Messages Into Codes

- Two basic approaches
  - Symmetric Key Algorithms (e.g., DES)
  - Asymmetric Key Algorithms (e.g., RSA)
- Both Types have strengthens & weaknesses

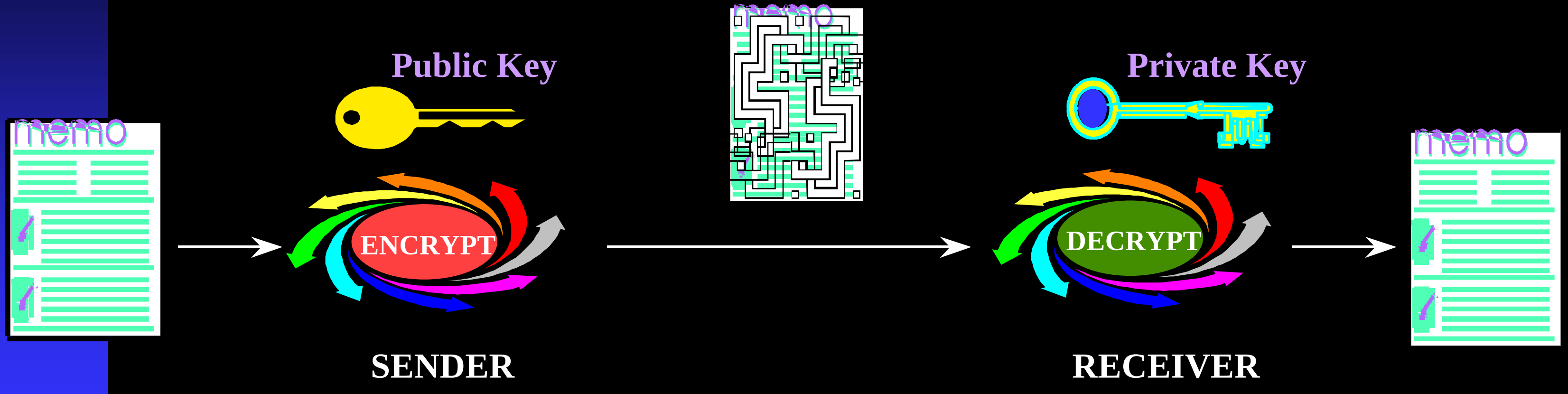
Symmetric Key Cryptography

- Also known as Secret Key Cryptography
- Based on a “shared” secret, known as the “key”.
- Strengths: Symmetric Cryptography is Fast
- Weaknesses: Key delivery and scalability



Asymmetric Key Cryptography

- Also known as Public Key Cryptography
- Based on using two different keys, a “public” key and a “private” key
- Strengths: Key delivery and scalability
- Weaknesses: Asymmetric Cryptography is Slow



Common Applications

- Symmetric (Secret) Key Cryptography
  - Privacy
  - Integrity - limited
- Asymmetric (Public) Key Cryptography
  - Authentication
  - Non-Repudiation (Digital Signature)
  - Key Exchange