

# CRYPTOGRAPHY



**PREPARED FOR**  
**COMPUTER SCIENCE DEPARTMENT**  
**UNIVERSITY OF MAKATI**

**BY**  
**RODEL URANI**

# Overview




- The magnitude of the whole security program
- The internetworking services and relevance of crypto
- The elements and characteristics added to security because of crypto
- Crypto Law in countries
- The processes involve in using crypto
- Security approaches may vary on scale

# Information Technology (IT)



- What is IT to you and your organization?
- How do you treat (or compare) IT with other communication medium?
  - Telephone – somebody says it is more direct
  - Telegram – somebody says urgency matters
  - Postal mail – somebody says it is more formal
- How do you define IT?
  - The resources to acquire, store, process and disseminate information<sup>1</sup>.

# Use of IT

A large, light grey semi-circle graphic on the left side of the slide, partially overlapping the text box.

The planning, design, development, deployment, operation, management and application of IT to meet the needs of the business. It includes both the demand for, and the supply of, IT services by internal business units, specialist IT units, or external suppliers and utility services.

# Magnitude of Security



- Controversial component of business-ICT program
- Effect to organization and individual can be fatal
- Entity's ICT coverage matter
- Stakeholders may need to collaborate diligently
- Planned and designed information infrastructure alone may assist in security

# Crypto Enabled Services



- Domain Name System Security Extension (DNSSEC)
  - .ORG Top Level Domain, signed roots June 2, 2009
- Internet Protocol Security (IPSec), Series of RFC's for SA, AH, ESP, et al
  - IP version 4 and 6
  - Virtual Private Network (VPN)
- Public Key Infrastructure (PKI) / Certificate Authority (CA)
  - Verisign, Thawte, Comodo

# Cryptosystems and Utilities



- OpenPGP (Pretty Good Privacy), RFC 4880
- Digital Rights Management (DRM)
- Private key cryptography
  - Blowfish
- Public key cryptography
  - RSA, Diffie-Hellman
- Hashing algorithm
  - MD5, SHA-2

# Crypto's Security Elements



- Integrity
- Confidentiality
- Authenticity
- Non-repudiation



# Crypto Law



- Wassenaar Arrangement
  - Export of arms and dual-use technology like crypto
  - 56-bit symmetric, 512-bit RSA (asymmetric) no longer export-controlled
- Survey of countries with import and export controls on crypto
  - By Dr. Bert-Jaap Koops (<http://rechten.uvt.nl/koops/cryptolaw>)

# Symmetric Process



## Sender's data

- Hello! This is a top secret message! Thanks.

Shared key

## Encrypted data

- # \$ % ^ & \*\*
- (LDL\*())\_+%

Shared key

## Recipient's data

- Hello! This is a top secret message! Thanks.

# Public Key Process



## Sender's data

- Hello, This is a top secret message! Thanks.

## Recipient's public key

## Encrypted data

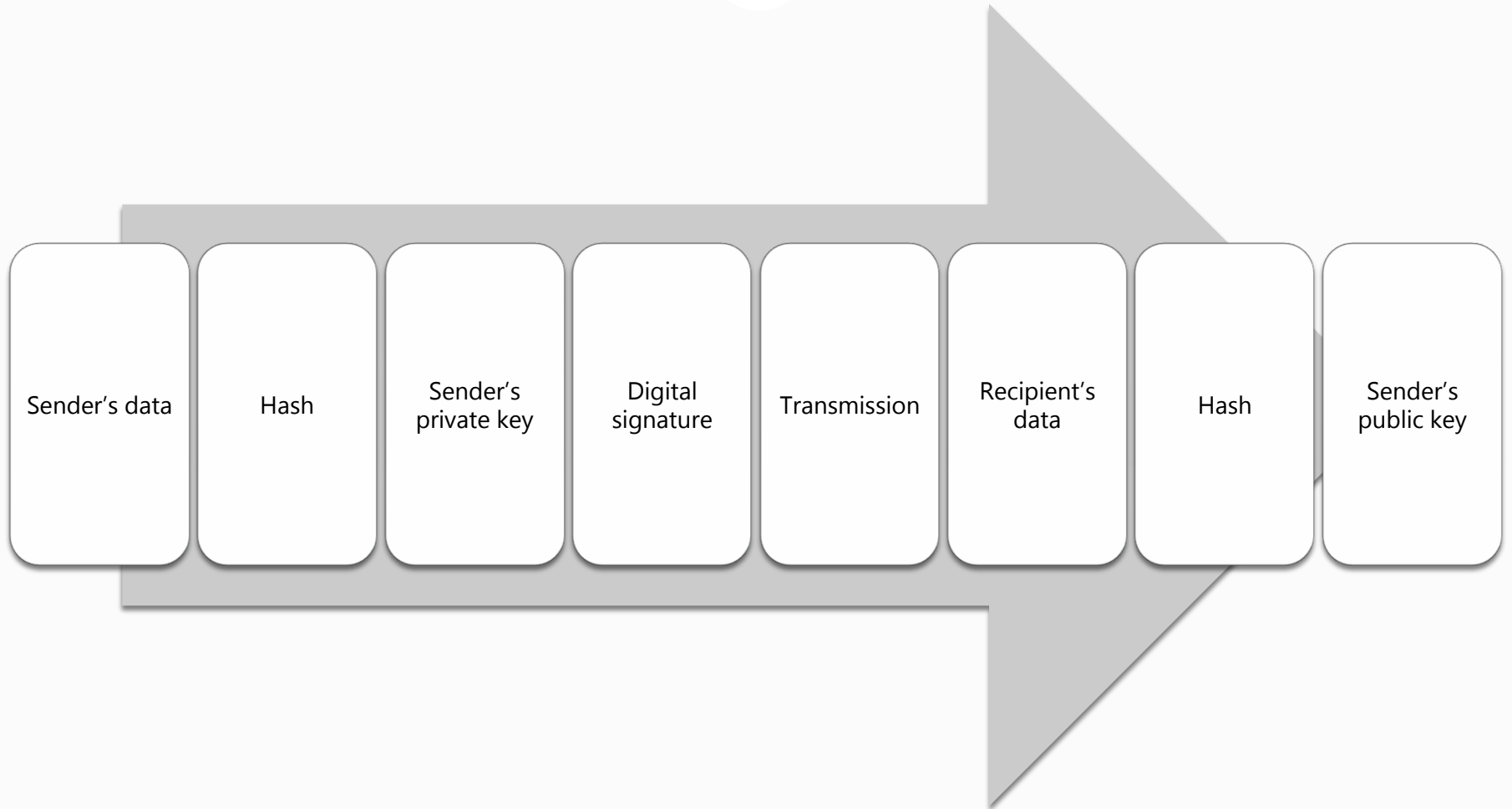
- !@#%^&89\*
- (!@@12345())
- ETAL

## Recipients private key

## Recipient's data

- Hello, This is a top secret message! Thanks.

# Digital Signature Process



# Security Efforts and Approaches



- Internet or cyber space
- Organization's internetworks
- Local network
- Individual computers connected to the Internet

Thank You!



# Q&A

Rodel @ Urani . tel