Cybersecurity for IoT – Fundamentals

Department of Electrical, Computer and Biomedical Engineering of University of Pavia

Master of Science Program in Computer Engineering

Instructor: Paris Kitsos

http://diceslab.cied.teiwest.gr

E-mail: pkitsos@teimes.gr

Pavia 2018

This lecture is based on “Cryptography and Network Security”, 4/e, book by William Stallings and

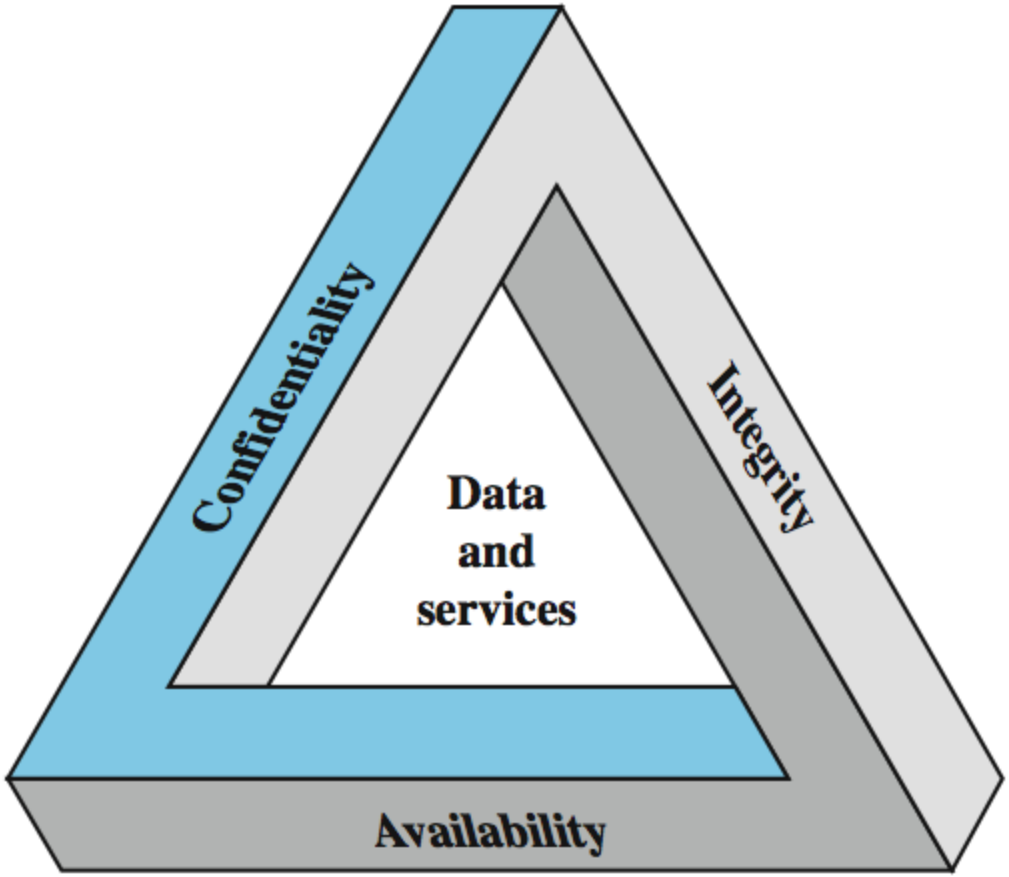
An extension chapter for “Understanding Cryptography — A Textbook for Students and Practitioners”, by Christof Paar and Jan Pelzl.

A Definition of Computer Security

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

- the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

Key Security Concepts…



…Key Security Concepts

- **Confidentiality:** Is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity :** Means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner
- **Availability:** Ensuring timely and reliable access to and use of information.

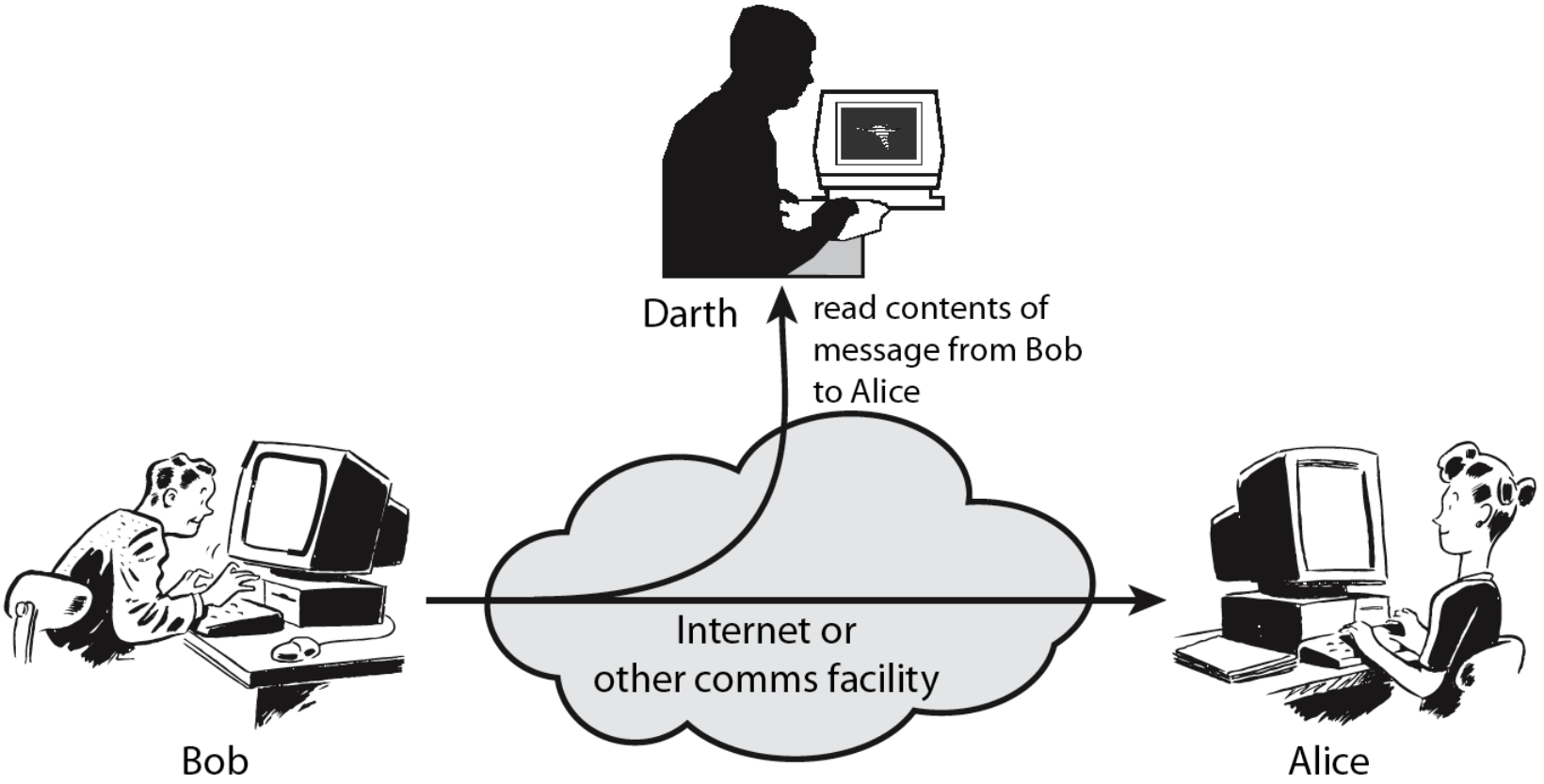
Security Attacks, Mechanisms and Services

- **Security attack**: Any action that compromises the security of information owned by an organization.

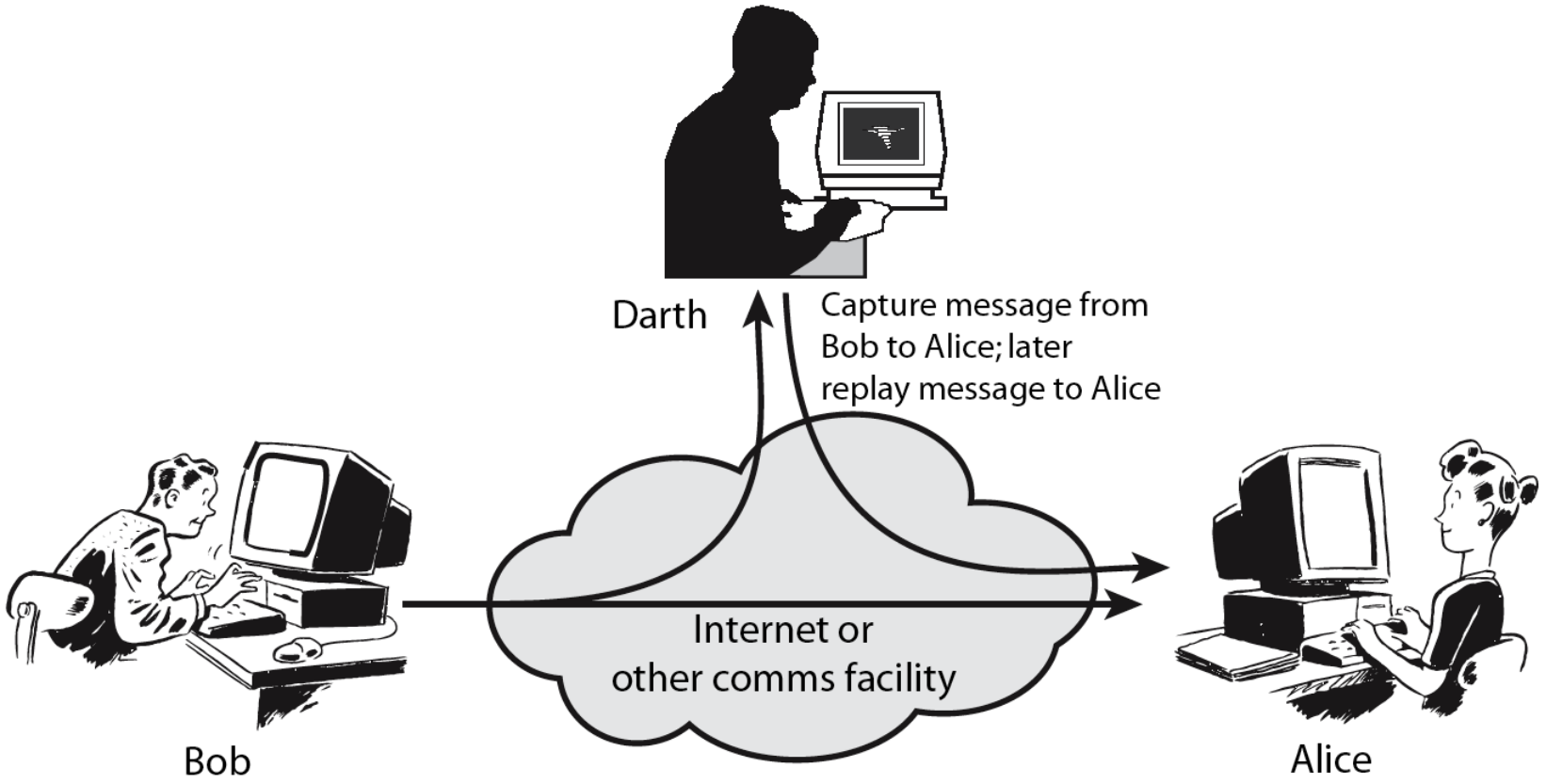
- **Security mechanism**: A process that is designed to detect, prevent, or recover from a security attack.

- **Security service**: A service that enhances the security of the data processing systems and the information transfers of an organization.

Passive Attack



Active Attack



Security Services

- Enhance security of data processing systems and information transfers of an organization
- Using one or more security mechanisms
- Needs a systematic way of defining the requirements of security
- Gives a way of organizing the tasks to provide security

Security Mechanisms

- Feature designed to detect, prevent, or recover from a security attack
- No single mechanism that will support all services required
- However one particular element underlies many of the security mechanisms in use:
  - –cryptographic techniques (Cryptography)

Cryptography [Wikipedia]

- Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries
- More generally, cryptography is about constructing and analyzing protocols in order to prevent third parties to read private messages

Encryption [Wikipedia]

- **Encryption**: is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.
- There are two types of Encryption
  - Symmetric encryption
  - Asymmetric encryption

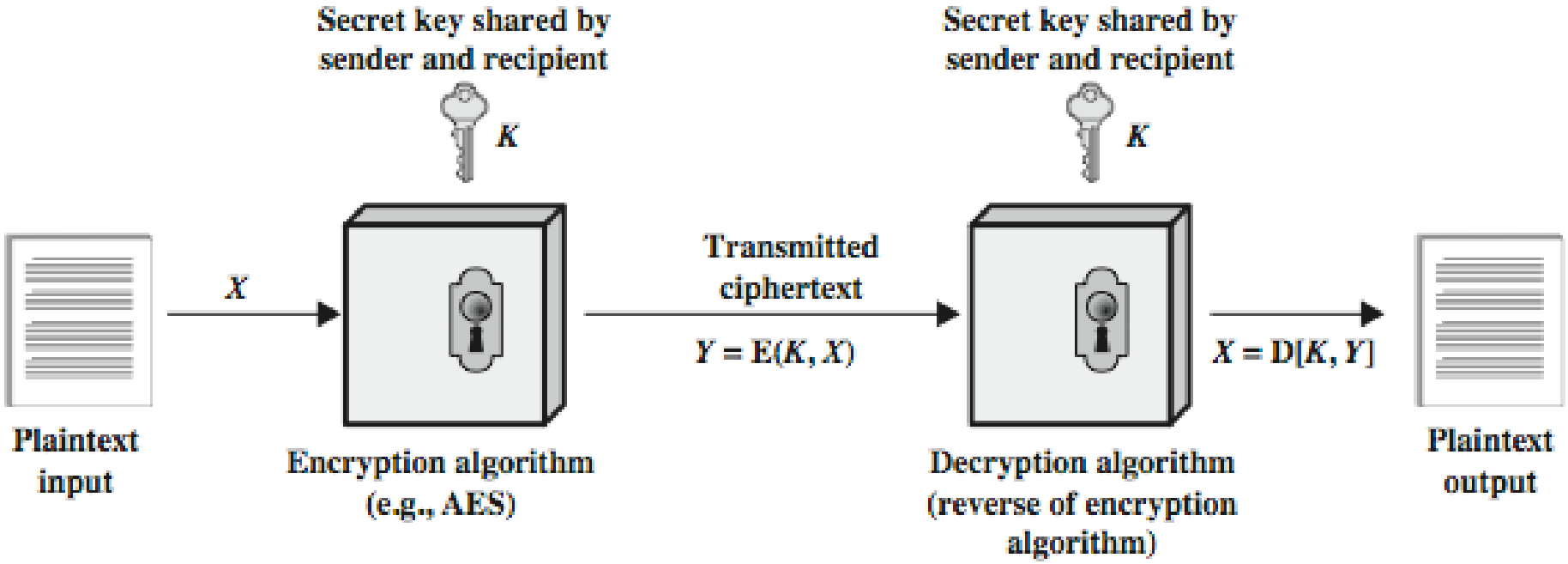
Symmetric Encryption

- or conventional / private-key / single-key
- Sender and receiver share a common key
- All classical encryption algorithms are private-key
- Was only type prior to invention of public-key in 1970's
- And by far most widely used

Basic Terminology

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encrypt** - converting plaintext to ciphertext
- **decrypt** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of decrypting ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

Symmetric Cipher Model



Basic Requirements

- There are two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- Mathematically have:

  $Y = E(K, X)$

  $X = D(K, Y)$
- Assume encryption algorithm is known
- Implies a secure channel to distribute key

Cryptanalysis

- Objective to recover key not just message
- A well known general approach
  - brute-force attack
- If either succeed all key use compromised

Brute Force Attack

- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognise plaintext

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56 (DES)	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128 (AES)	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168 (Triple-DES)	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years

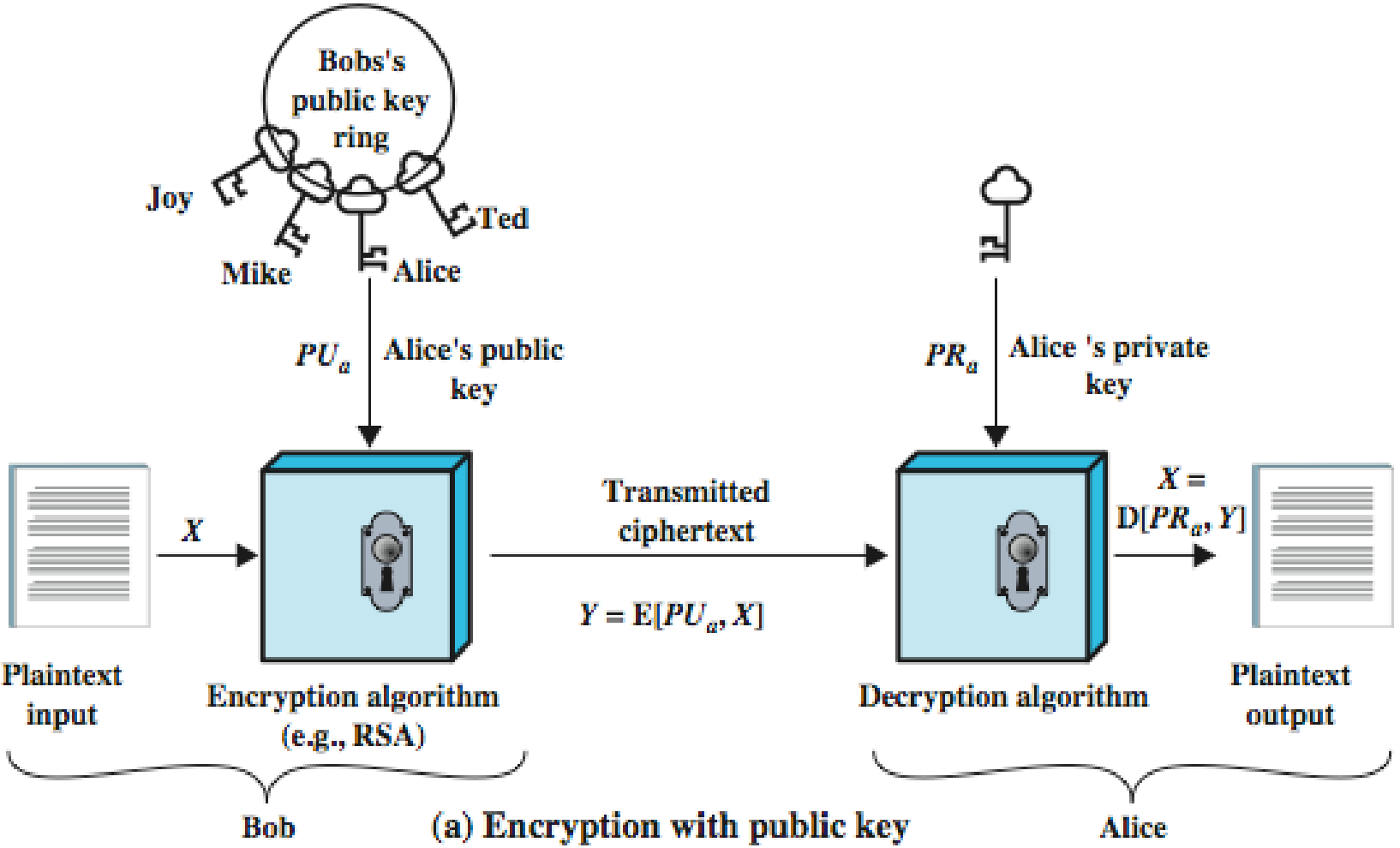
Asymmetric encryption

- Uses **two** keys – a public & a private key
- **Asymmetric** since parties are **not** equal
- Uses clever application of number theoretic concepts to function
- Complements **rather than** replaces private key crypto

Public Key Cryptography…

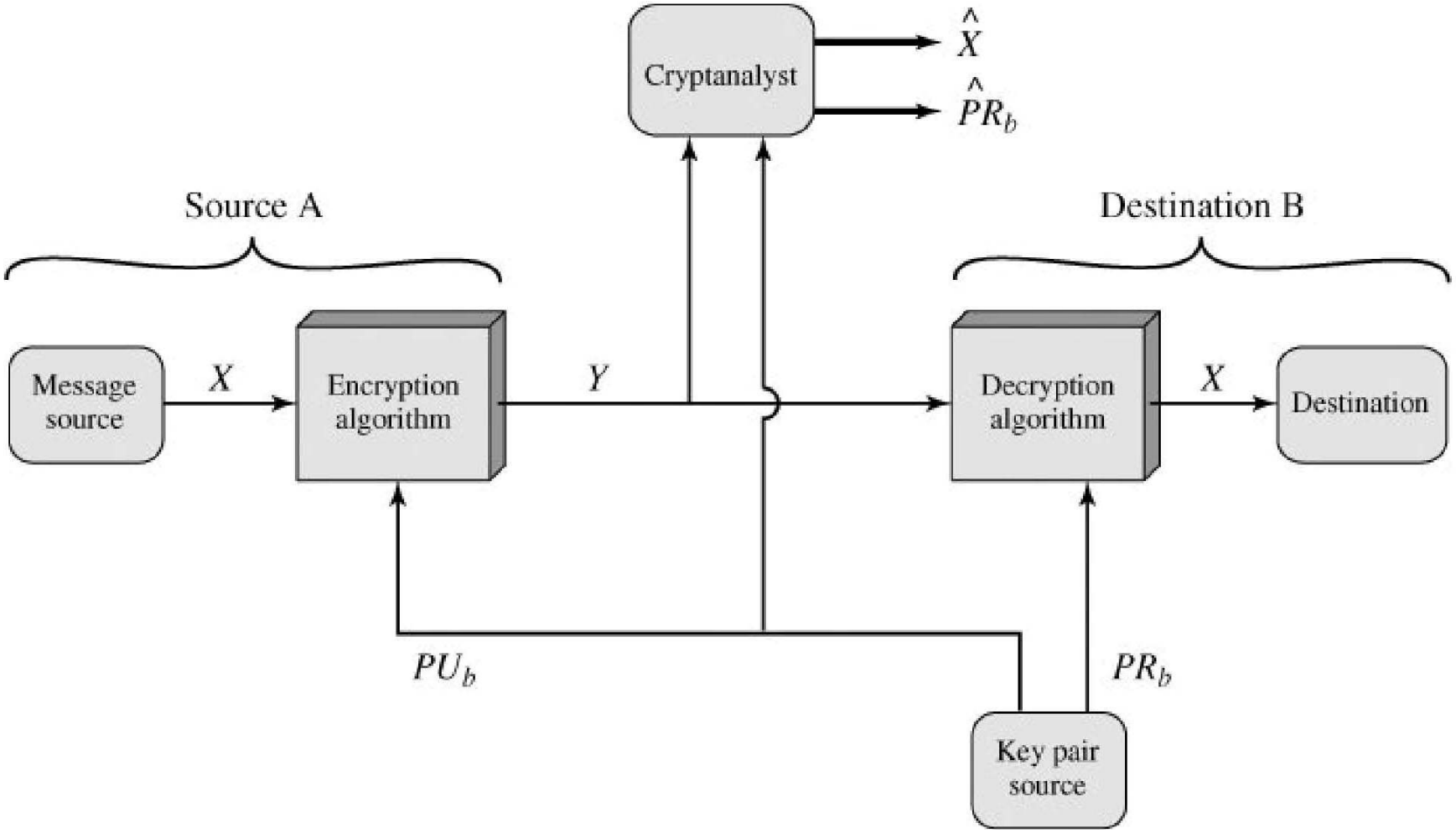
- **Public-key/two-key/asymmetric** cryptography involves the use of **two** keys:
  - a **public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**
  - a related **private-key**, known only to the receiver, used to **decrypt messages**, and **sign** (create) **signatures**
- **Infeasible to determine private key from public**
- Is **asymmetric** because
  - those who encrypt messages or verify signatures **cannot** decrypt messages or create signatures

…Public Key Cryptography…



(a) Encryption with public key

…Public Key Cryptography



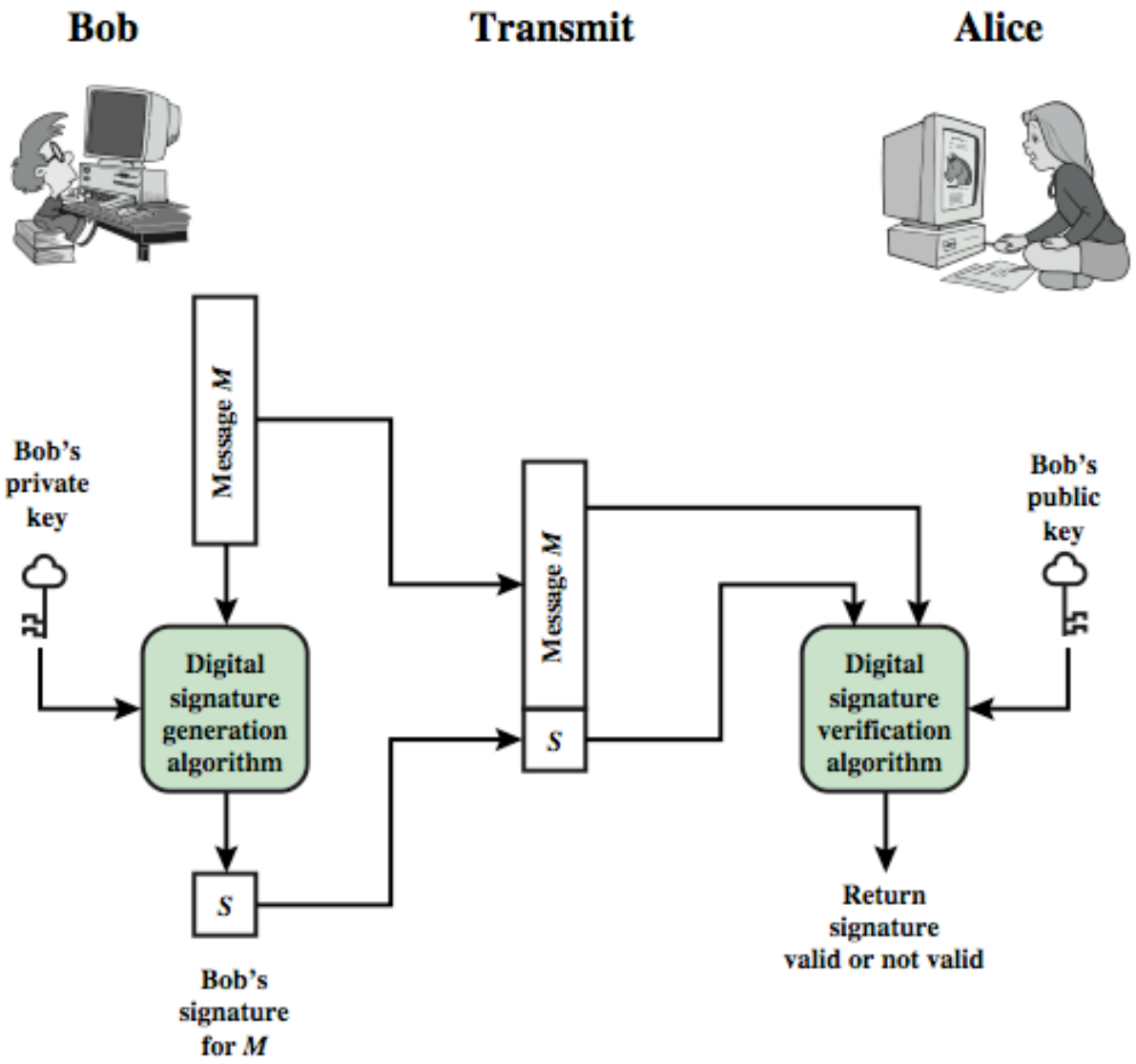
Symmetric Vs Asymmetric Cryptography

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

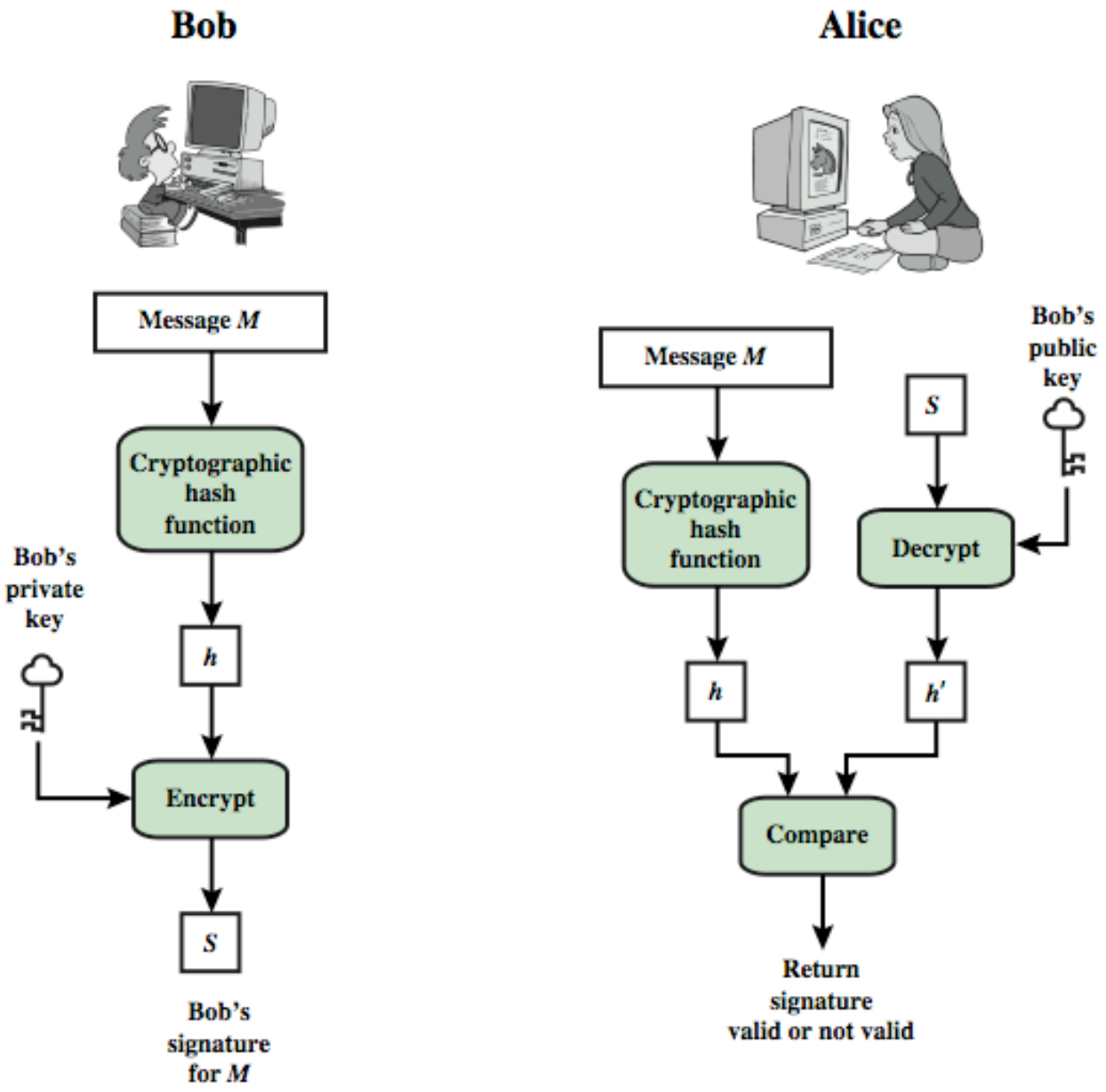
Digital Signatures

- Have looked at message authentication
  - but does not address issues of lack of trust
- Digital signatures provide the ability to:
  - verify author, date & time of signature
  - authenticate message contents
- Hence include authentication function with additional capabilities

Digital Signature Model



Digital Signature Model



Message Authentication

- message authentication is concerned with:
  - protecting the integrity of a message
  - validate the identity of originator
- the three alternative functions used:
  - hash function
  - message encryption
  - message authentication code (MAC)

Hash Functions

- condenses arbitrary message to fixed size

  `h = H(M)`

- usually assume hash function is public
- hash used to detect changes to message
- want a cryptographic hash function
  - computationally infeasible to find data mapping to specific hash (one-way property)
  - computationally infeasible to find two data to same hash (collision-free property)

Hash Function Requirements

Requirement	Description
Variable input size	H can be applied to a block of data of any size.
Fixed output size	H produces a fixed-length output.
Efficiency	H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
Preimage resistant (one-way property)	For any given hash value h, it is computationally infeasible to find y such that H(y) = h.
Second preimage resistant (weak collision resistant)	For any given block x, it is computationally infeasible to find y ! x with H(y) = H(x).
Collision resistant (strong collision resistant)	It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).
Pseudorandomness	Output of H meets standard tests for pseudorandomness

Secure Hash Algorithm

- SHA (SHA-0) originally designed by NIST & NSA in 1993
- was revised in 1995 as SHA-1
- US standard for use with DSA signature scheme
  - standard is FIPS 180-1 1995, also Internet RFC3174
- produces 160-bit hash values
- recent 2005 results on security of SHA-1 have raised concerns on its use in future applications

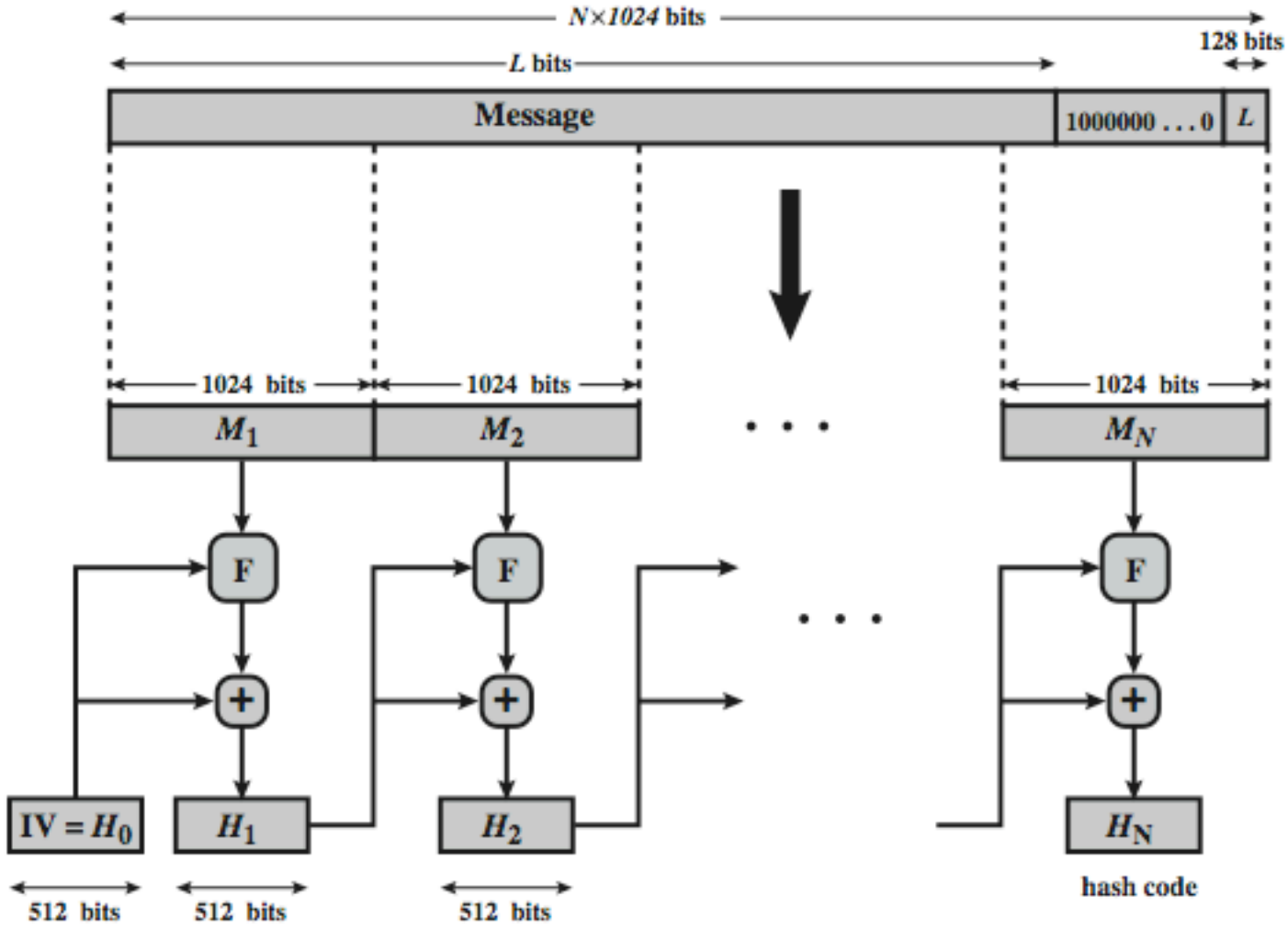
Revised Secure Hash Standard

- NIST issued revision FIPS 180-2 in 2002
- adds 3 additional versions of SHA
  - SHA-256, SHA-384, SHA-512
- designed for compatibility with increased security provided by the AES cipher
- structure & detail is similar to SHA-1
- hence analysis should be similar
- but security levels are rather higher

SHA Versions

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message digest size	160	224	256	384	512
Message size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block size	512	512	512	1024	1024
Word size	32	32	32	64	64
Number of steps	80	64	64	80	80

SHA-512 Overview



SHA-512 Compression Function

- heart of the algorithm
- processing message in 1024-bit blocks
- consists of 80 rounds
  - updating a 512-bit buffer
  - using a 64-bit value Wt derived from the current message block
  - and a round constants

SHA-3…

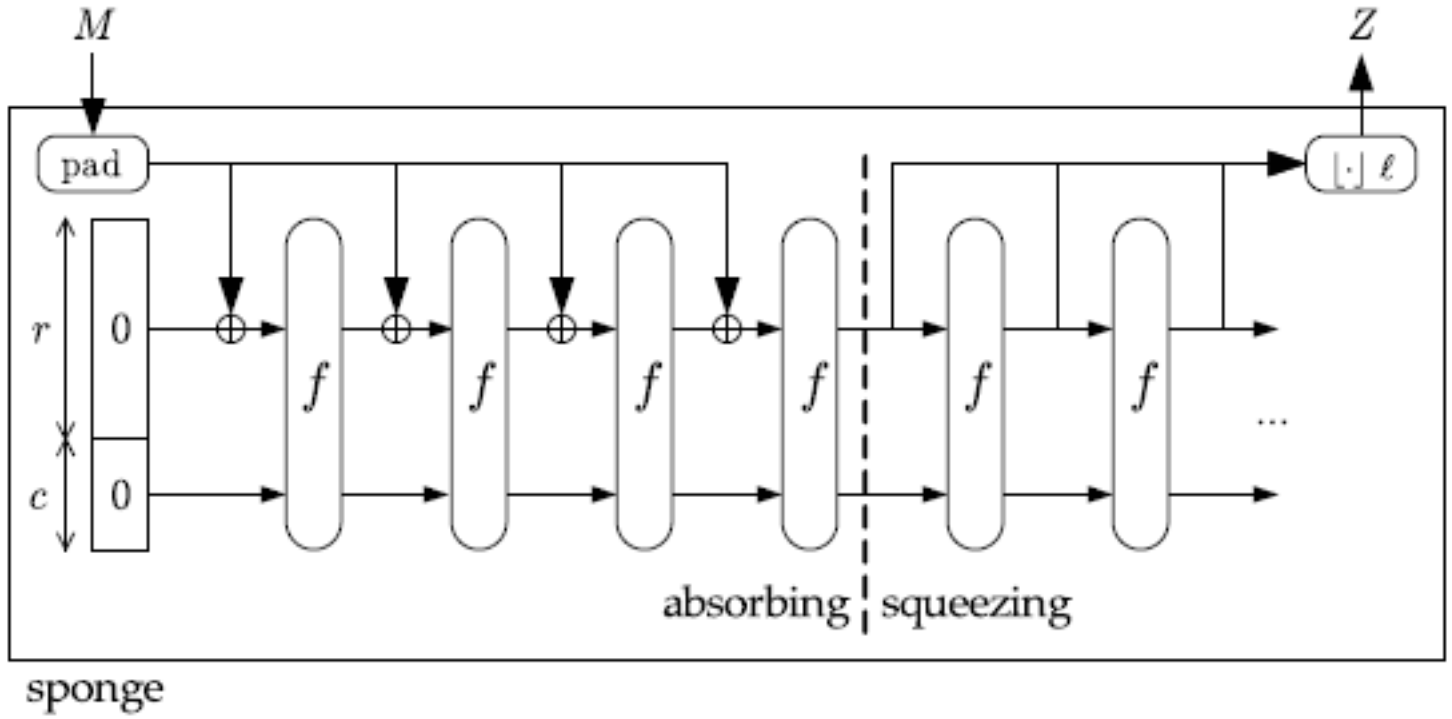
- In 2006 NIST started to organize the NIST hash function competition to create a new hash standard, SHA-3.
- SHA-3 is not meant to replace SHA-2, as no significant attack on SHA-2 has been demonstrated.
- Because of the successful attacks on SHA-0 and SHA-1, NIST perceived a need for an alternative, dissimilar cryptographic hash, which became SHA-3.

…SHA-3

- 51 candidates were submitted by the end of 2008.
- In July 2009, 14 algorithms were selected for the second round.
- NIST selected five SHA-3 candidate algorithms to advance to the third (and final) round.
- And finally, selects Keccak as SHA-3 standard.

Keccak Hash Function…

- Keccak uses the sponge construction, in which data is "absorbed" into the sponge.
- And the result is "squeezed" out.

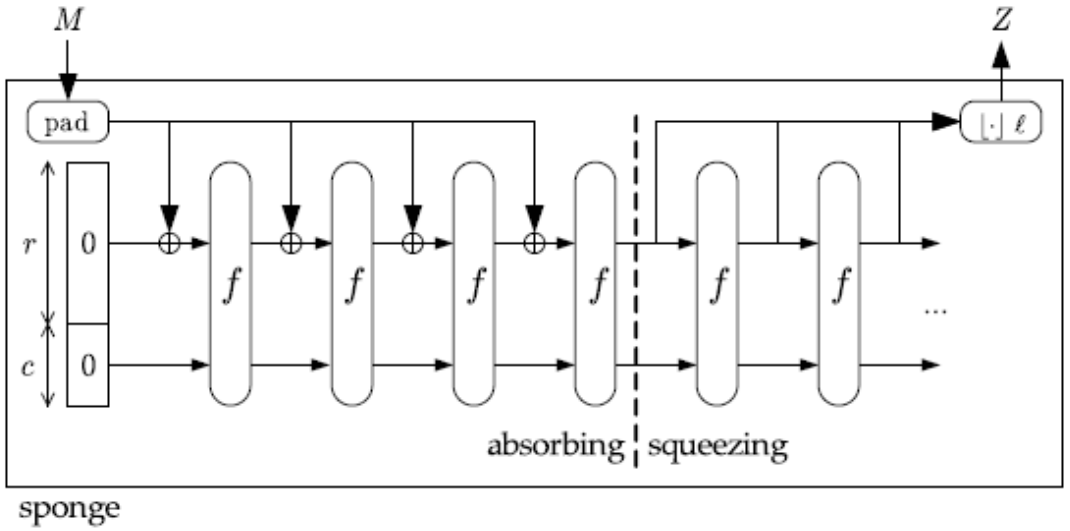


[From Wikipedia]

…Keccak Hash Function…

- In the “absorbing” phase, message blocks are XORed into a subset of the state, which is then transformed as a whole using a permutation function f.
- In the “squeeze” phase, output blocks are read from the same subset of the state, alternated with the state transformation function f.

…Keccak Hash Function…



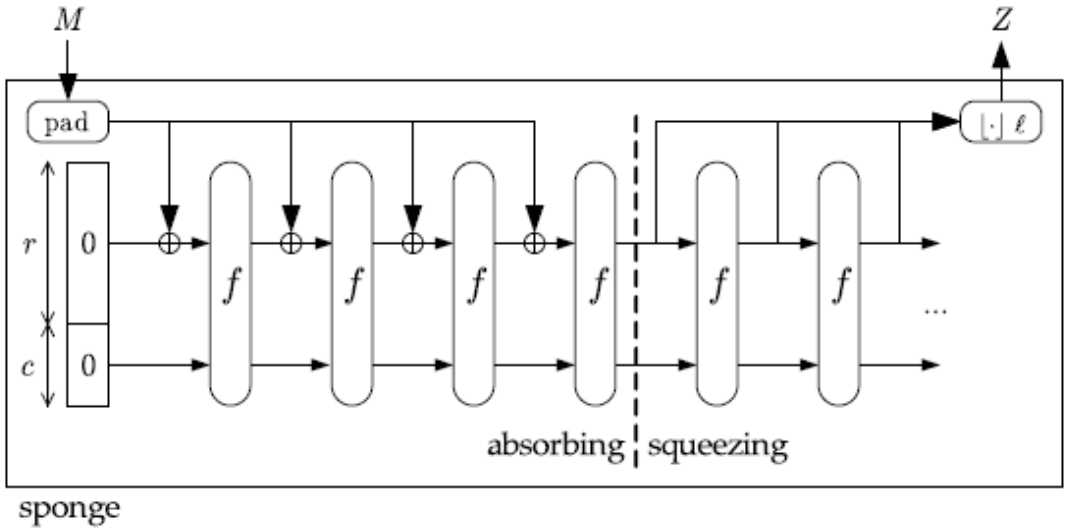
- M: message (input)
- c: capacity
- r : rate

- Z: digest (output)
- l is the output length
- f: permutation of b = r + c bits

…Keccak Hash Function…

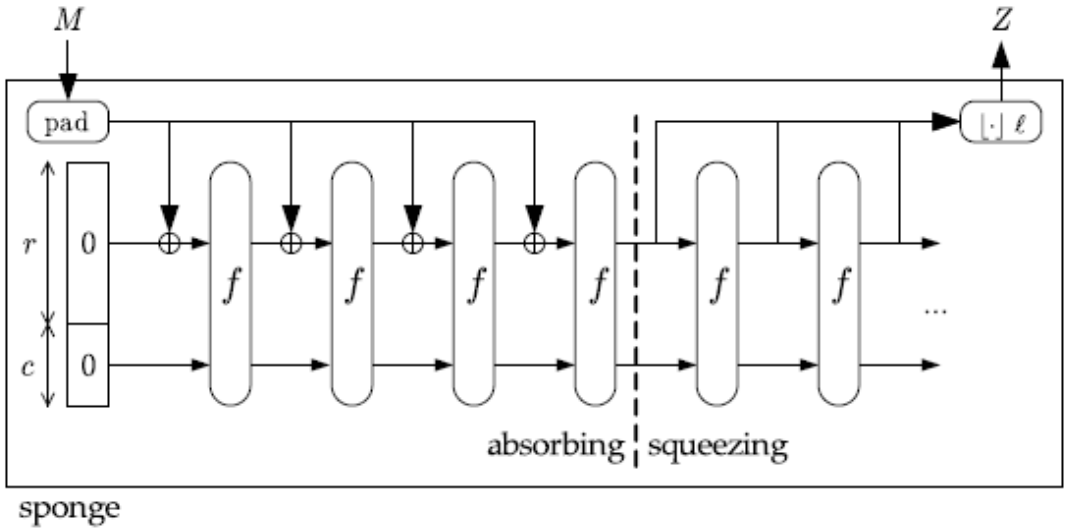
- The size of the part of the state that is written and read is called the "rate" (denoted r),
- The size of the part that is untouched by input/output is called the "capacity" (denoted c).
  - The capacity determines the security of the scheme.

…Keccak Hash Function…



- The message is padded to form a multiple of r -bit blocks
- Absorbing phase: At each step r -bits of the message are XORed to r bits of the state
- When we finish to process the message we change to the squeezing phase
- Squeezing phase: At each step r -bits of the state are output to form the digest

…Keccak Hash Function…



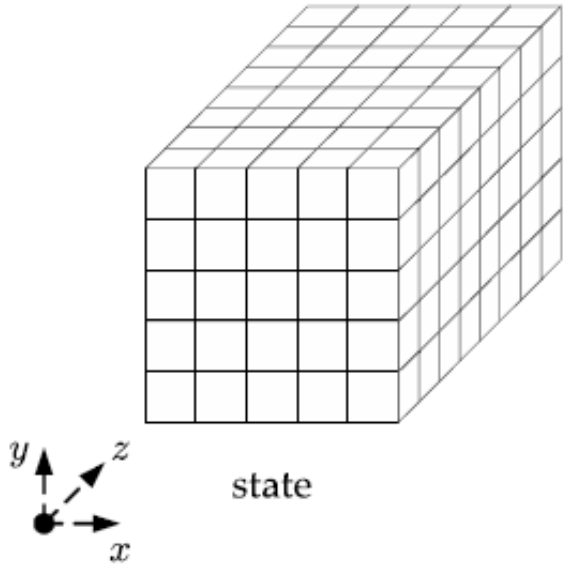
Name	ℓ	c	r
SHA3-224	224	448	1152
SHA3-256	256	512	1088
SHA3-384	384	768	832
SHA3-512	512	1024	576

- In all these versions c + r = 1600

…Keccak Hash Function…

State A

- Description of the 1600-bit permutation
- 5 x 5 x 64 bits
- Each square =1 bit
- $0 \leq x, y \leq 4, 0 \leq z \leq 63$
- Can be represented by 25 integer values

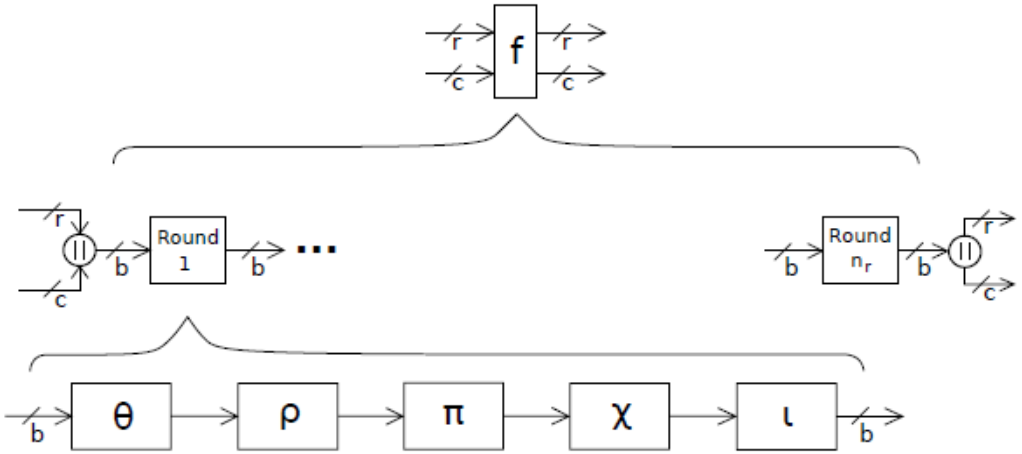


…Keccak Hash Function…

- Round function (f)

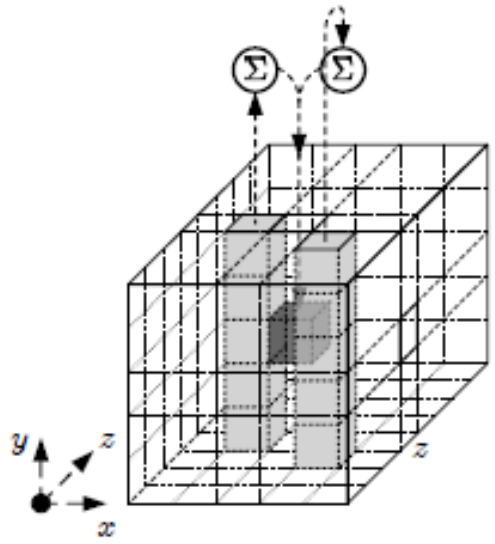
- The f function: 24 rounds
- 1 round: Given the state A and the round index ir

  $Rnd(A,ir) = \iota_{ir} \circ \chi \circ \pi \circ \rho \circ \Theta(A)$



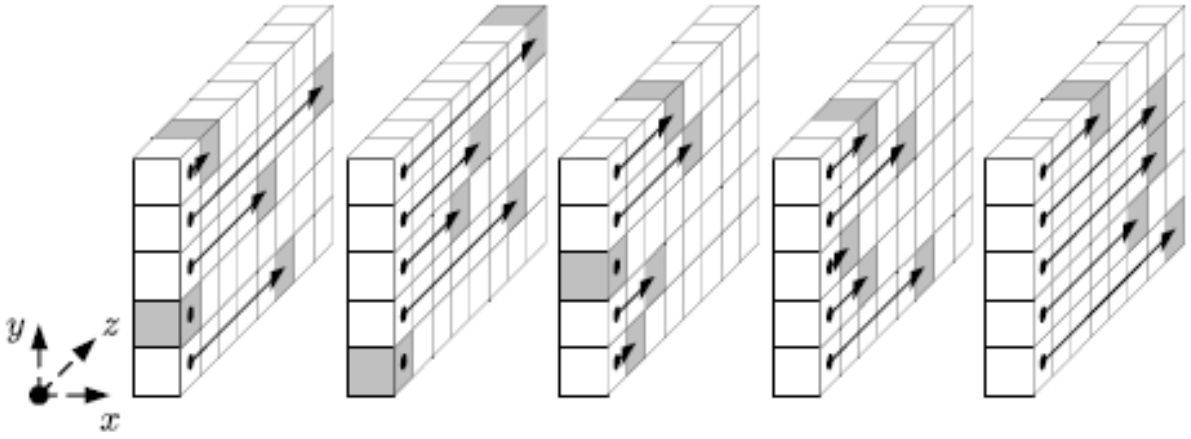
…Keccak Hash Function…

- Θ function
- Sum all columns
- Add the sum of 2 columns (x - 1; z) (x + 1; z - 1) to a bit value (x; y; z)



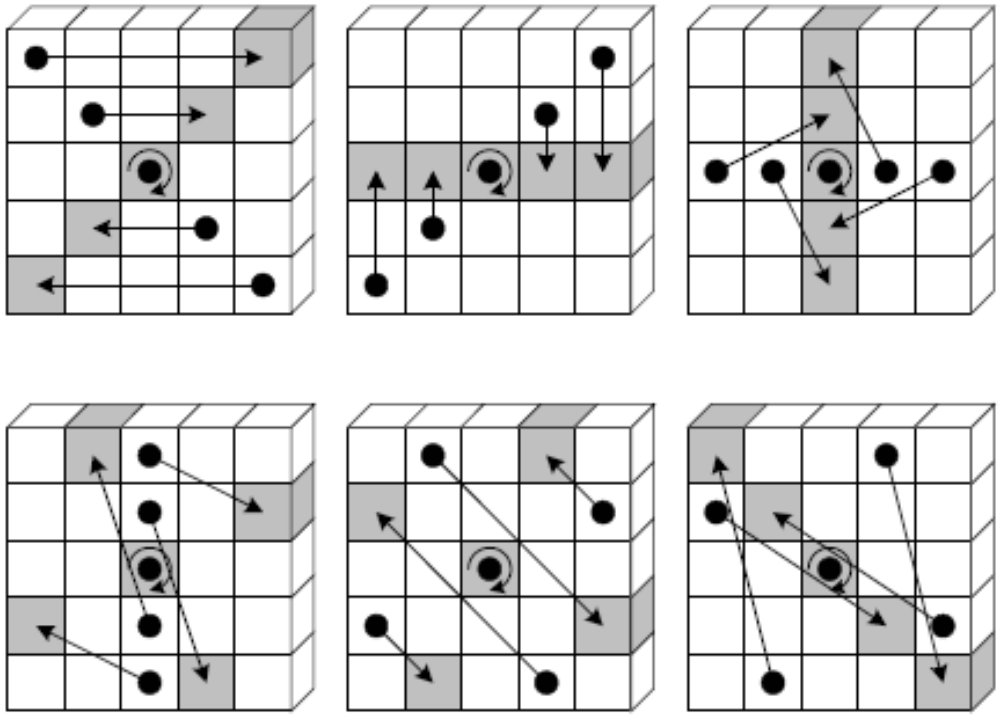
…Keccak Hash Function…

- ρ function
- Rotate each lane by a given value (25 lanes)



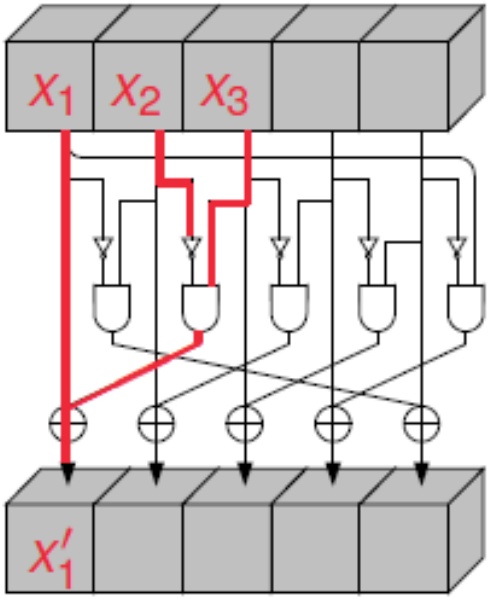
…Keccak Hash Function…

- π function
- Rearrange the positions of the lanes



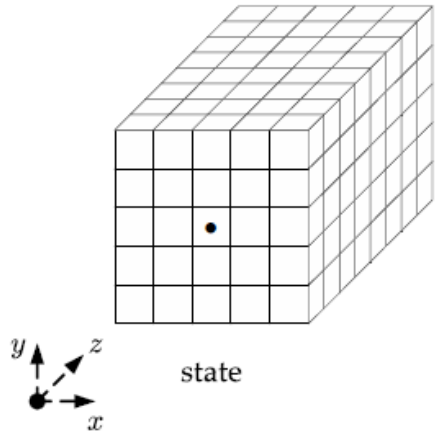
…Keccak Hash Function…

- x function
- XOR each bit with a non-linear function of two other bits in its row
- For example, $x_1' <- x_1 + x_2 x_3$
- Behave like a 5-bit Sbox



…Keccak Hash Function…

- ι function
- Modify some of the bits of Lane (0, 0) in a manner that depends on the round index ir
- If the lanes are represented as 64-bit integer, this step consists of a XOR with the round constant.



…Keccak Hash Function

- More details about Keccak in the page: http: //nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

Questions??