CY 411 Reverse Software Engineering

Review of Cryptography

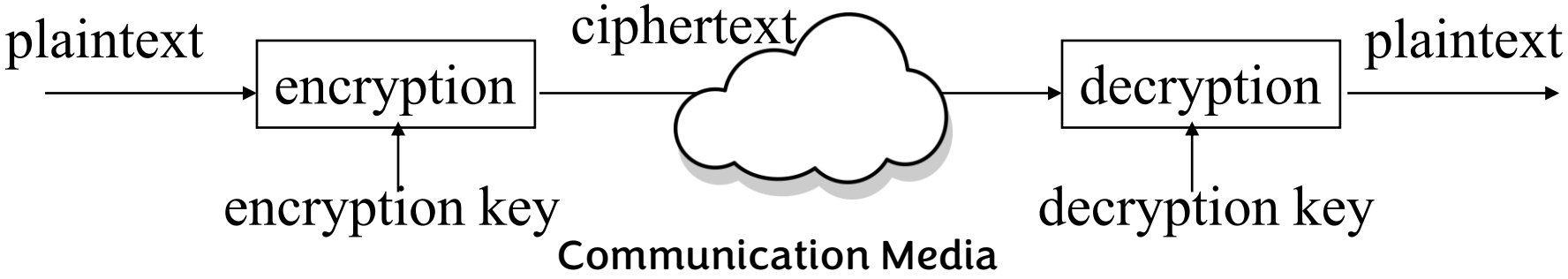
Dr. Qasem Abu Al-Haija

Department of Cybersecurity
Faculty of Computer & Information Technology
Jordan University of Science and Technology

Cryptography

- Cryptography
  - Original meaning: The art of secret writing
  - Becoming a science that relies on mathematics (number theory, algebra)
  - Process data into unintelligible form, reversible, without data loss
  - Usually, one-to-one

Encryption/Decryption



- Plaintext: a message in its original form
- Ciphertext: a message in the transformed, unrecognized form
- Encryption: the process that transforms a plaintext into a ciphertext
- Decryption: the process that transforms a ciphertext to the corresponding plaintext
- Key: the value used to control encryption/decryption

Cryptanalysis (algorithms are known)

- Definition: Assume the encryption/decryption algorithms are known. Get the keys
- Ciphertext only:
  - Analyze only with the ciphertext
  - Example: Exhaustive search until "recognizable plaintext"
  - Smarter ways available
- Known plaintext:
  - Secret may be revealed (by spy, time). Thus <ciphertext, plaintext> pair is obtained
- Chosen plaintext:
  - Choose text, get encrypted
  - Useful if limited set of messages

Security of An Encryption Algorithm

Unconditionally secure

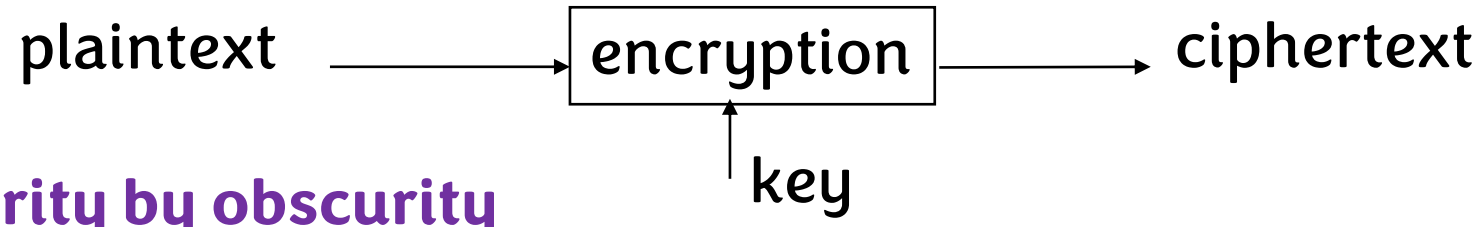
- It is impossible to decrypt the ciphertext
- One-time pad (the key is as long as the plaintext)

$$C_i = P_i \oplus k_i$$

Computationally secure

- The cost of breaking the cipher exceeds the value of the encrypted information
- The time required to break the cipher exceeds the useful lifetime of the information

Secret Keys v.s. Secret Algorithms



Security by obscurity

- We can achieve better security if we keep the algorithms secret
- Hard to keep secret if used widely
- Reverse engineering, social engineering
- Example: in the Military world, Keep algorithms secret (Avoid giving enemy good ideas). The military has access to the public domain knowledge anyway.

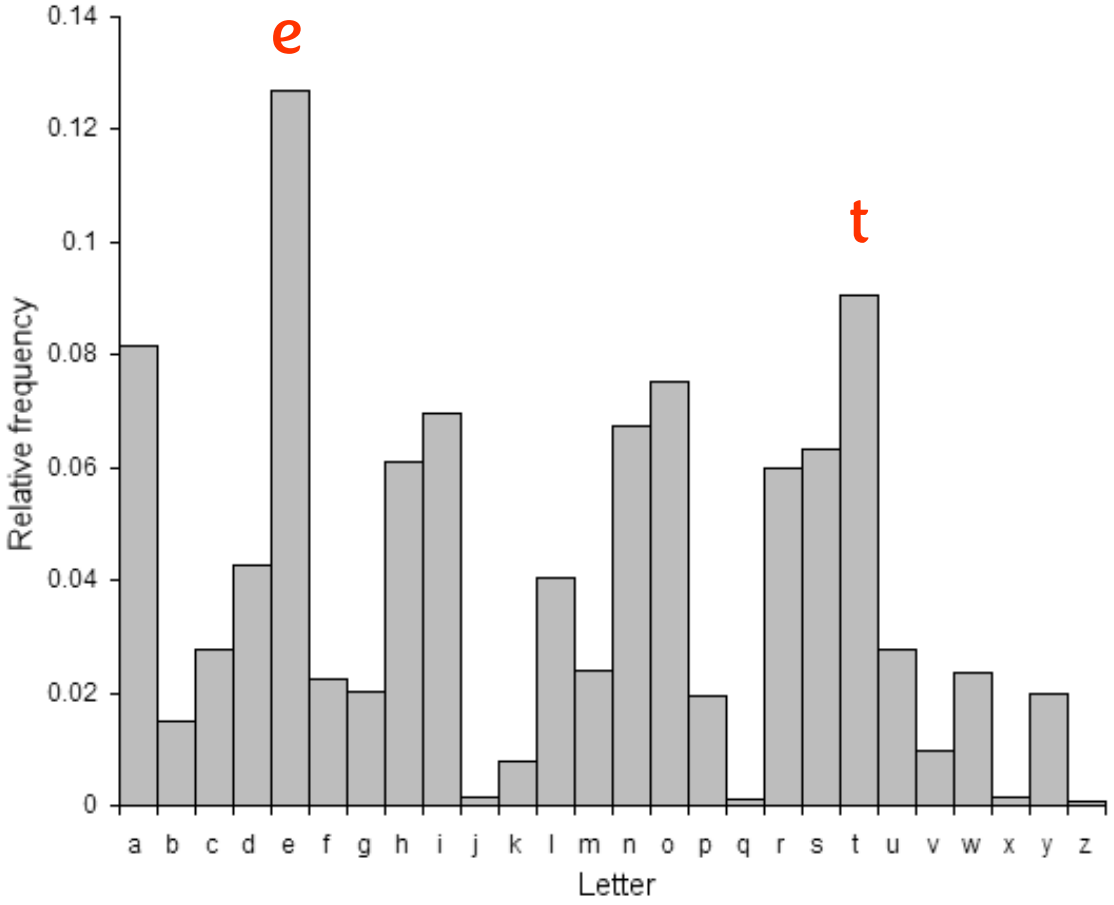
Publish the algorithms

- Security of the algorithms depends on the secrecy of the keys
- Less unknown vulnerability if all the smart (good) people in the world examine the algorithms
- Example: In the Commercial world, we publish the algorithm (Wide review, trust)

Some Trivial Codes

Some Trivial Codes

- Mono-alphabetic cipher:
  - Arbitrary mapping of one letter to another
  - 26!
  - Statistical analysis of letter frequencies



http://en.wikipedia.org/wiki/Letter_frequencies

Some Trivial Codes (Cont.)

- Caesar cipher
  - Substitution cipher
  - Replace each letter with the one 3 letters later
  - A $\rightarrow$ D, B $\rightarrow$ E

x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

- hello
- khoor

Captain Midnight Secret Decoder Rings

only 26 possibilities

Some Trivial Codes (Cont.)

a	0	e	4	i	8	m	12	q	16	u	20	y	24
b	1	f	5	j	9	n	13	r	17	v	21	z	25
c	2	g	6	k	10	o	14	s	18	w	22		
d	3	h	7	l	11	p	15	t	19	x	23		

- Affine Cipher
  - Encoding letters as numbers [0, 25]
  - $E_{a,b}(x)=(ax+b)\%26$; (a,b) is the key
    - Reduction modulo N%m: $N=qm+r$, $0 \le r < m$; 7%6=?
    - $E_{3,11}(a)$=?
  - Multiple round affine cipher $E_{a,b}(E_{a,b}(E_{a,b}(x)))$

Some Trivial Codes (Cont.)

- Poly-alphabetic Ciphers
  - A letter may be encrypted into different letters from time to time

Some Trivial Codes (Cont.)

- All the previous codes are based on substitution
- Transposition (permutation) – Columnar Transposition

1. Write in rows of fixed length
2. Read column by column in a scrambled order

Key	4	3	1	2	5	6	7
Plaintext:	A	T	T	A	C	K	P
	O	S	T	P	O	N	E
	D	U	N	T	I	L	T
	W	O	A	M	X	Y	Z

- Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Columnar Transposition

- Plaintext

Z	E	B	R	A	S
6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	Q	K	J	E	U

The permutation (transposition) is defined by the alphabetical order of the letters within the keyword

- EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE

One time pad

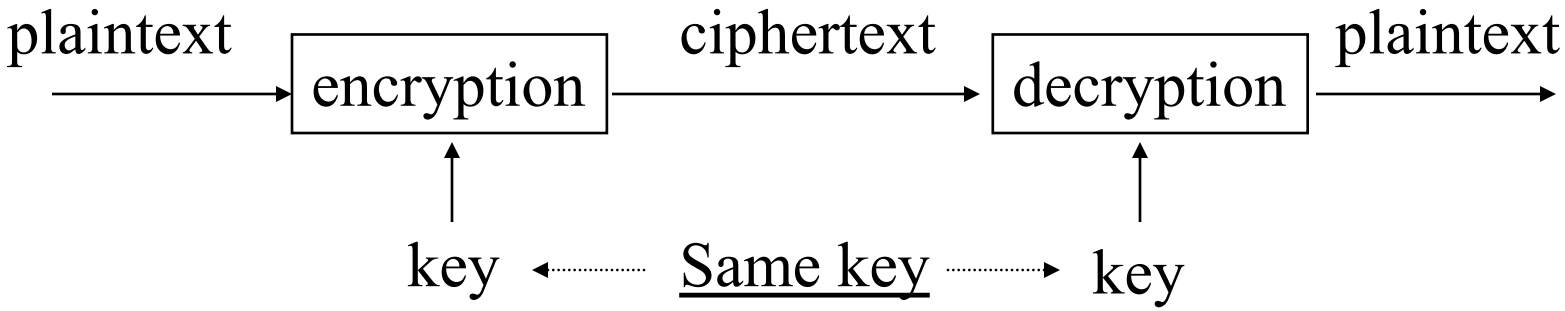
- $E(x_1|...|x_n)=(x_1+k_1)\%26|...|(x_n+k_n)\%26$
- Where is it used?

Types of Cryptography and their Applications

Types of Cryptography

- Number of keys
  - Hash functions: no key
  - Secret key cryptography: one key
  - Public key cryptography: two keys – public, private
- The way in which the plaintext is processed
  - Block cipher: divides input elements into blocks
  - Stream cipher: process one element (e.g., byte) a time

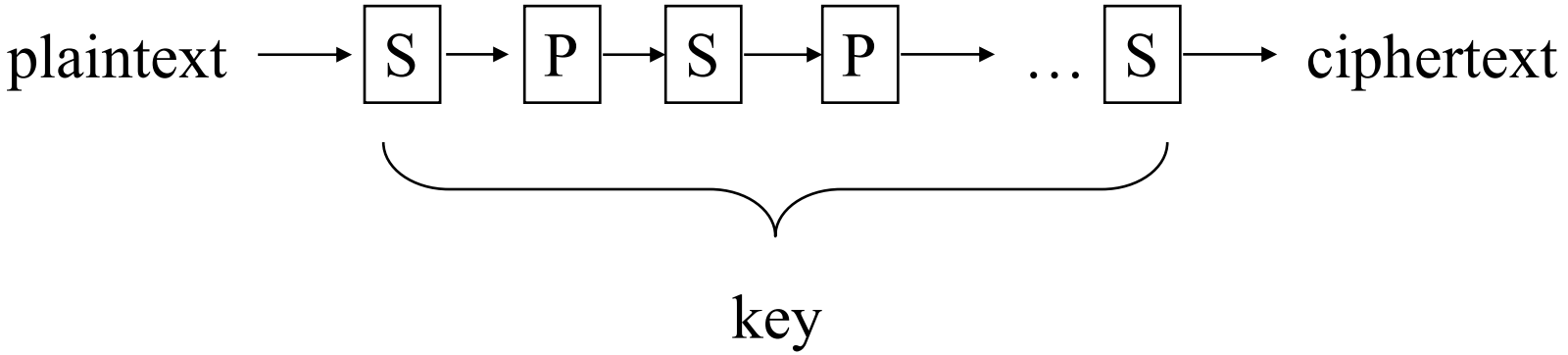
Secret Key Cryptography



- Same key is used for encryption and decryption
- Also known as
  - Symmetric cryptography
  - Conventional cryptography

Secret Key Cryptography (Cont.)

- Basic technique
  - Product cipher
  - Multiple applications of interleaved substitutions and permutations



Secret Key Cryptography (Cont.)

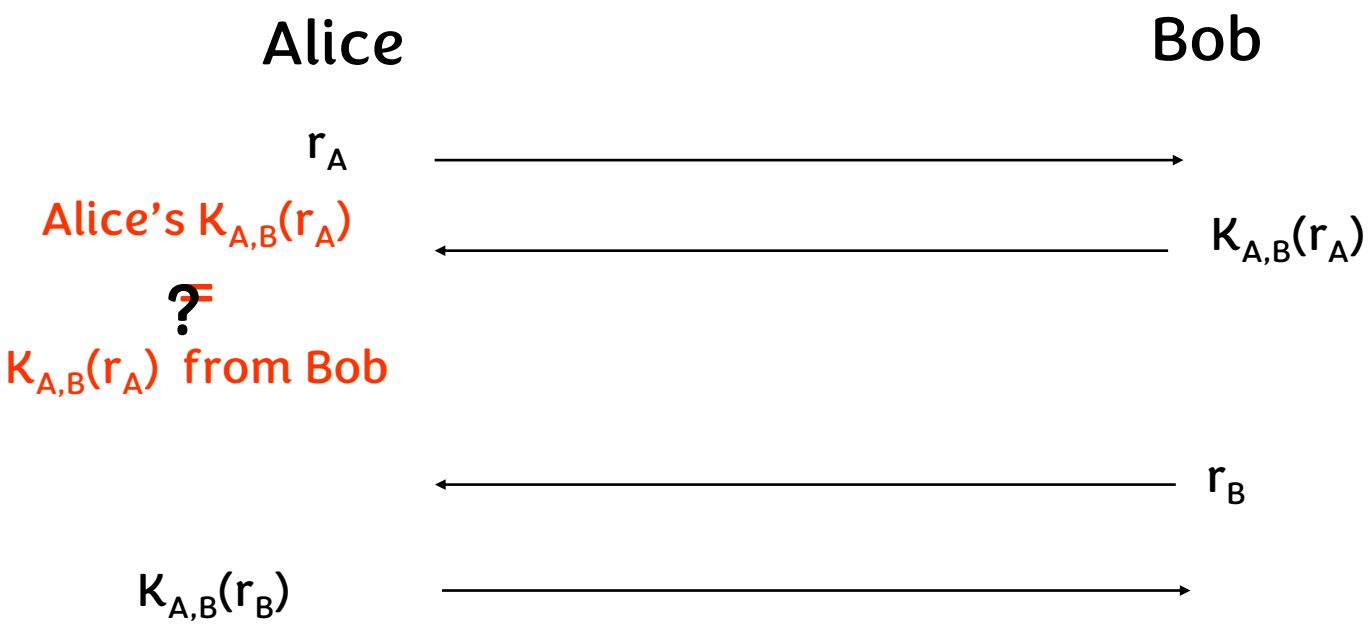
- Ciphertext approximately the same length as plaintext
- Examples
  - Stream Cipher: RC4
  - Block Cipher: DES, 3DES, IDEA, AES

Applications of Secret Key Cryptography

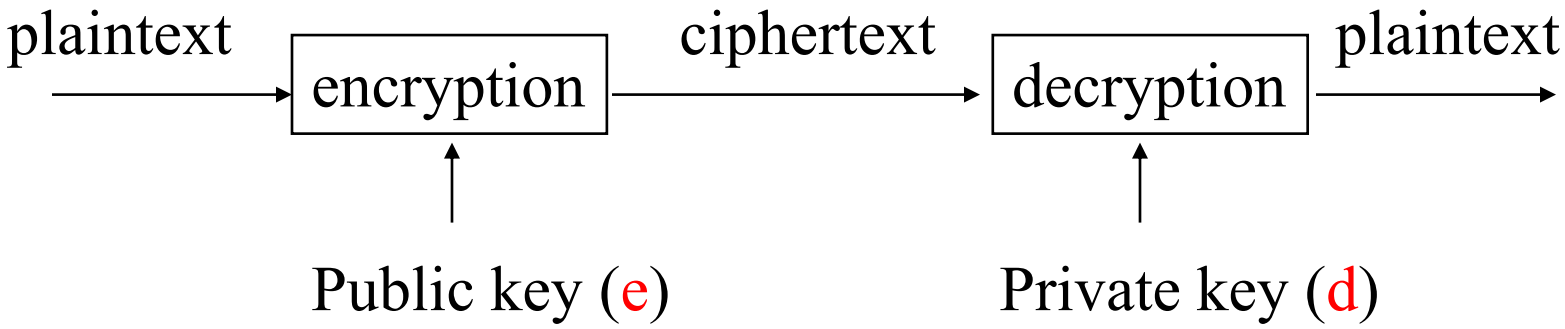
- Transmitting over an insecure channel
  - Challenge: How to share the key?
- Secure Storage on insecure media
- Integrity check
  - Message integrity code (MIC)

Authentication Using Secret Key Cryptography

- Challenge-response
- To prove the other party knows the secret key
- Must be secure against chosen plaintext attack



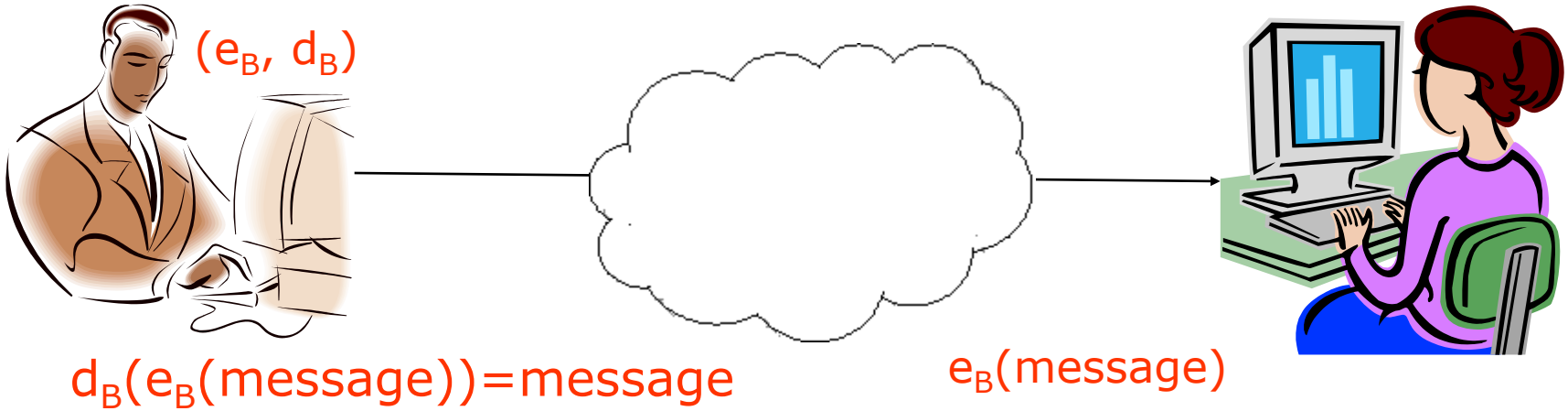
Public Key Cryptography



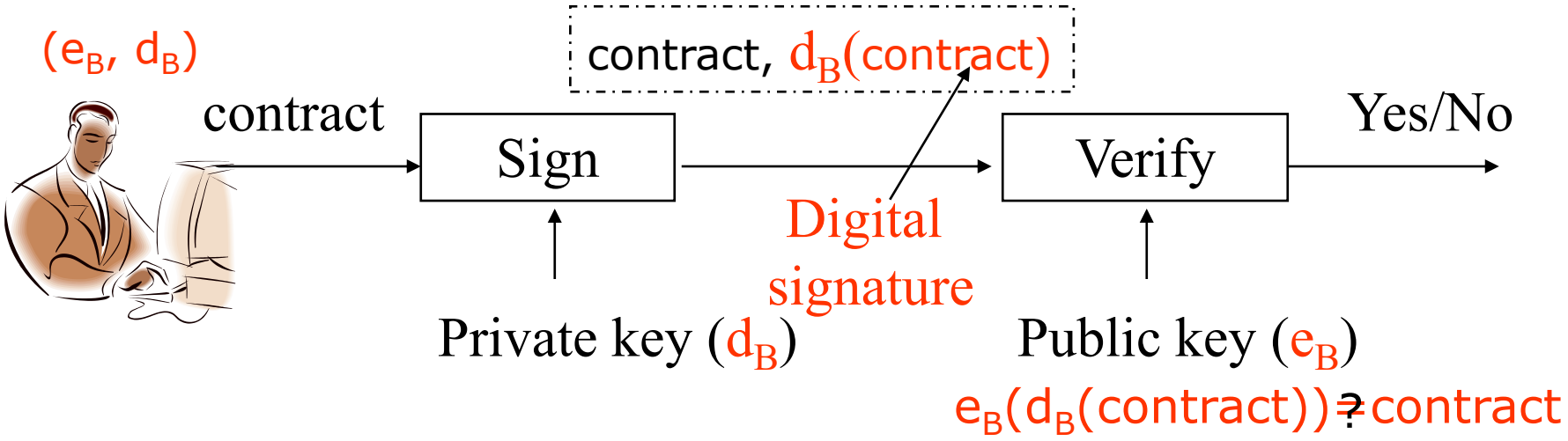
- Invented/published in 1975 (?)
- A public/private key pair is used
  - Public key can be publicly known
  - Private key is kept secret by the owner of the key
- Much slower than secret key cryptography
- Also known as
  - Asymmetric cryptography

Applications of Public Key Cryptography

- Data transmission:
  - Alice encrypts m_a using Bob's public key e_B, Bob decrypts m_a using his private key d_B
- Storage:
  - Can create a safety copy: using public key of trusted person



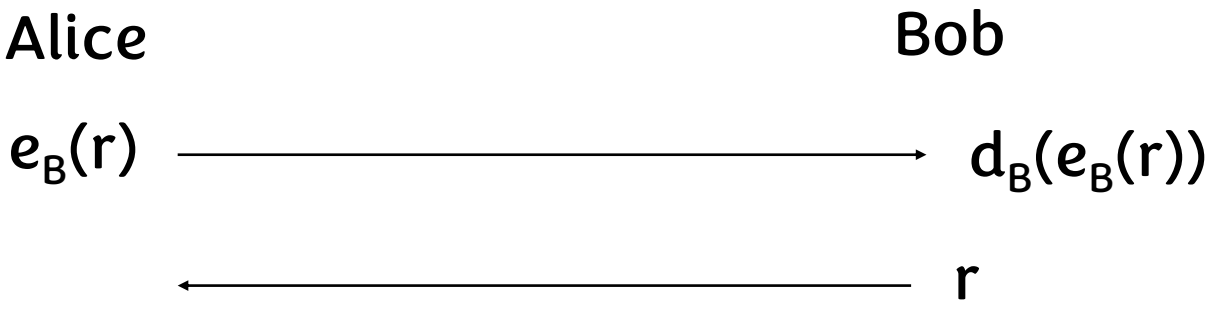
Naive digital signature



- Only the party with the private key can create a digital signature
- The digital signature is verifiable by anyone who knows the public key
- The signer cannot deny that he/she has done so

Authentication Using Public Key Cryptography

- No need to store secrets, only need public keys
- Secret key cryptography: need to share secret key for every person to communicate with



Applications of Public Key Cryptography (Cont.)

- Key exchange
  - Establish a common session key between two parties

Hash Algorithms

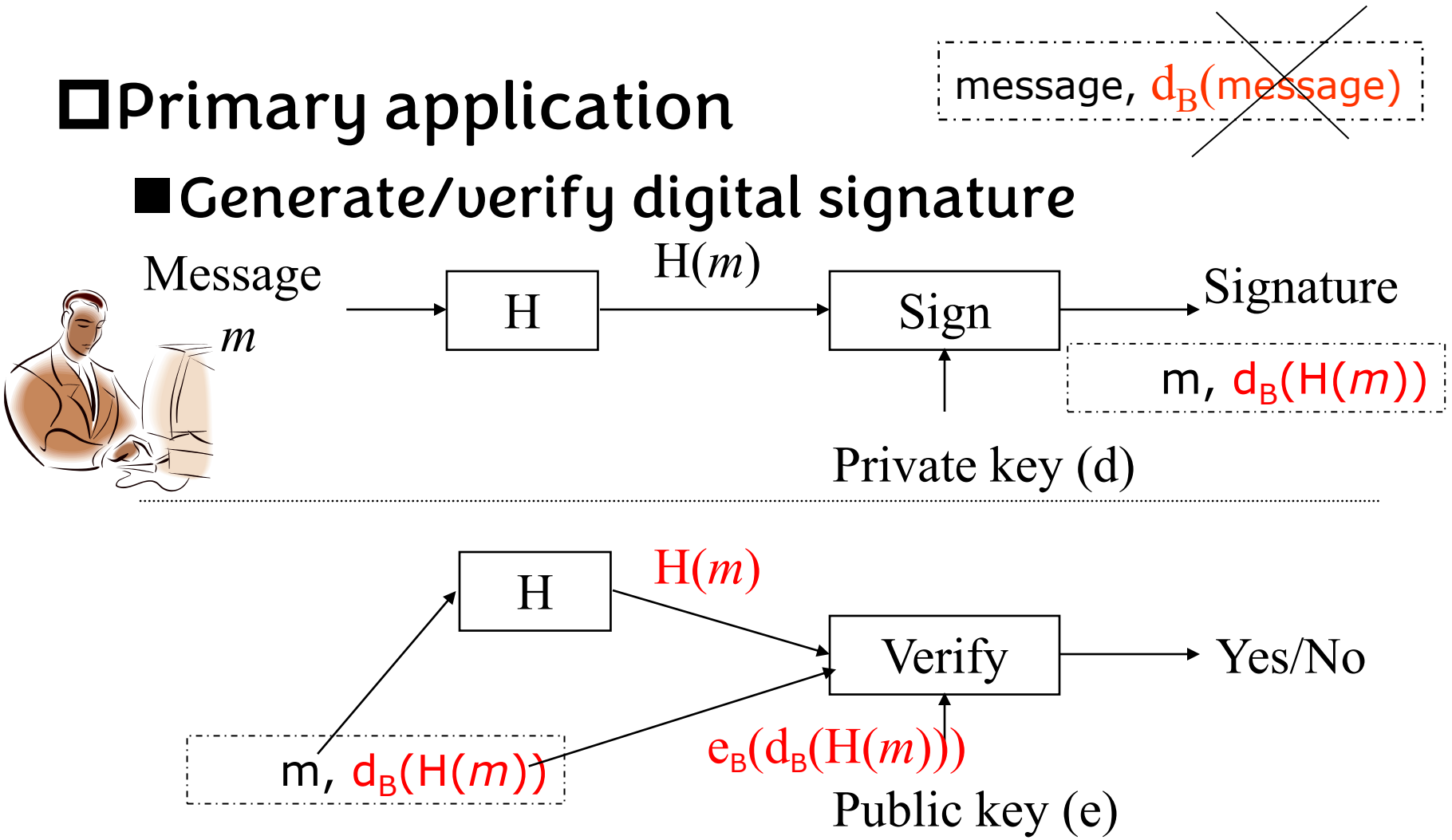
- Also known as
  - Message digests
  - One-way transformations
  - One-way functions
  - Hash functions
- Length of $H(m)$ much shorter then length of m
- Usually fixed lengths: 128 or 160 bits (16 bytes or 20 bytes)

Hash Algorithms (Cont.)

- Desirable properties of hash functions
  - Performance: Easy to compute $H(m)$
  - One-way property: Given $H(m)$ but not m, it's difficult to find m
  - Weak collision free: Given $H(m)$, it's difficult to find m' such that $H(m') = H(m)$.
  - Strong collision free: Computationally infeasible to find m_1, m_2 such that $H(m_1) = H(m_2)$

Applications of Hash Functions

- Primary application
  - Generate/verify digital signature



Applications of Hash Functions (Cont.)

- Password hashing
  - Doesn't need to know password to verify it
  - Store $H(password|salt)$ and salt, and compare it with the user-entered password
  - Salt makes dictionary attack more difficult
- Message integrity
  - Keyed hash
    - Agree on a secret key k
    - Compute $H(m|k)$ and send with m
  - But doesn't require encryption algorithm, so the technology is exportable