Computer Network Security , ITC502, M1L2

Classical Encryption Techniques

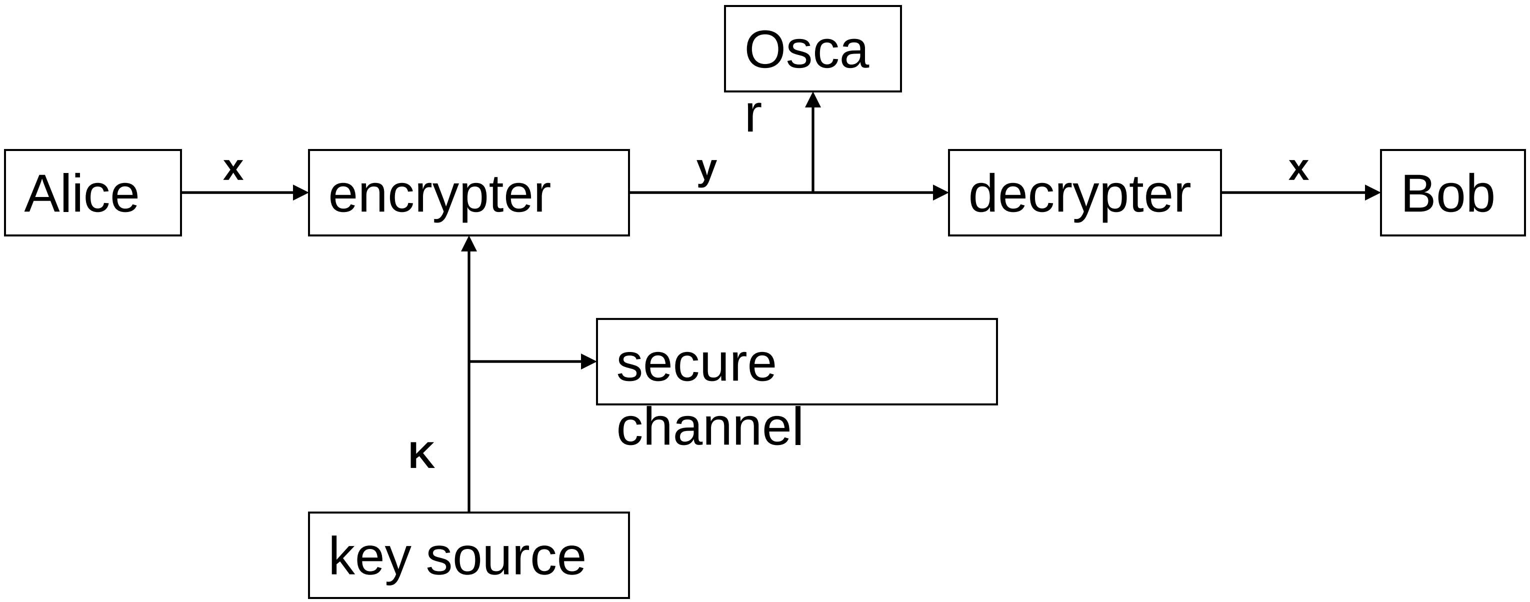
Introduction:
Some Simple Cryptosystems

Outline

- [1] Introduction: Some Classical Simple Cryptosystems
  - <1> The Shift Cipher
  - <2> The Substitution Cipher
  - <3> The Affine Cipher
  - <4> The Vigenère Cipher
  - <5> The Hill Cipher
  - <6> The Permutation Cipher
  - <7> Stream Ciphers
- [2] Cryptanalysis
  - <1> Cryptanalysis of the Affine Cipher
  - <2> Cryptanalysis of the Substitution Cipher
  - <3> Cryptanalysis of the Vigenère Cipher
  - <4> Cryptanalysis of the Hill Cipher
  - <5> Cryptanalysis of the LFSR Stream Cipher

Introduction:
Some Simple Cryptosystems

- [1] Introduction



Introduction: Some Simple Cryptosystems

- Definition 1.1: A cryptosystem is a five-tuple $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ satisfies
  - $\mathcal{P}$ is a finite set of possible *plaintexts*
  - $\mathcal{C}$ is a finite set of possible *ciphertexts*
  - $\mathcal{K}$, the *keyspace*, is a finite set of possible *keys*
  - For each $K\in\mathcal{K}$, there is an encryption rule $e_K\in\mathcal{E}$ and a corresponding decryption rule $d_K\in\mathcal{D}$
    - $$e_K : \mathcal{P} \rightarrow \mathcal{C}$$
      $$d_K : \mathcal{C} \rightarrow \mathcal{P}$$
    - $d_K(e_K(x))=x$ for every plaintext $x\in\mathcal{P}$

Introduction: Some Simple Cryptosystems

- Definition 1.2: a and b are integers,

  m is a positive integer

  - congruence: $a \equiv b \pmod{m}$ if m divides b-a

- Z_m: the set {0,1,…,m-1}

  - with 2 operations + and $\times$
  - $10+20=4$ in Z_{26} $(10+20 \bmod 26=4)$
  - $10\times 20=18$ in Z_{26} $(10\times 20 \bmod 26=18)$

Introduction: Some Simple Cryptosystems

- <1> Shift Cipher **(Caesar Cipher)**
  - Cryptosystem 1.1: Shift Cipher
    - $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26}$
    - $K, x, y \in Z_{26}$
    - $e_K(x) = (x+K) \bmod 26$
    - $d_K(y) = (y-K) \bmod 26$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Introduction: Some Simple Cryptosystems

- eg.: Suppose K=11
  - Plaintext: student
  - Ciphertext: DEFOPZE

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

plaintext	s	t	u	d	e	n	t
	18	19	20	3	4	13	19
+K	3	4	5	14	15	25	4
ciphertext	D	E	F	O	P	Z	E

K=5, 17, information technology

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Introduction: Some Simple Cryptosystems

- <2> Substitution Cipher
  - Cryptosystem 1.2: Substitution Cipher
    - $P=C=Z_{26}$
    - K: all possible permutations of the 26 symbols
    - For each $\pi \in \mathcal{K}$
      - $e_\pi(x)=\pi(x)$
      - $d_\pi(y)=\pi^{-1}(y)$

    where π^{-1} is the inverse permutation to π

Introduction: Some Simple Cryptosystems

- eg.:

x	a	b	C	d	e	f	g	h	i	j	k	l	m
$e_\pi(x)$	X	N	Y	A	H	P	O	G	Z	Q	W	B	T
x	n	o	p	q	r	s	t	u	v	w	x	y	z
$e_\pi(x)$	S	F	L	R	C	V	M	U	E	K	J	D	I

- Plaintext: student, information, your name
- Ciphertext: VMUSHSM , ZSPFCTXMZFS , ?

Introduction: Some Simple Cryptosystems

- <3> Affine Cipher
  - Theorem 1.1: $ax \equiv b \pmod m$ has a unique solution $x \in Z_m$ for every $b \in Z_m$ iff $\gcd(a,m)=1$
  - Definition 1.3: Suppose $a \geq 1$ and $m \geq 2$ are integers
    - a and m are *relatively prime* if $\gcd(a,m)=1$
    - $\phi(m)$: the number of integers in Z_m that are relatively prime to m

$$m = \prod_{i=1}^{n} p_i^{e_i}$$

  - Theorem 1.2: Suppose

$$\phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1})$$

Introduction: Some Simple Cryptosystems

- Definition 1.4: Suppose $a \in Z_m$
  - $a^{-1} \bmod m$:

    the multiplicative inverse of a modulo m
  - $aa^{-1} \equiv a^{-1}a \equiv 1 \pmod{m}$
- Cryptosystem 1.3: Affine Cipher
  - $\mathcal{P} = \mathcal{C} = Z_{26}$
  - $\mathcal{K} = \{(a,b) \in Z_{26} \times Z_{26} : \gcd(a,26)=1\}$
  - For $K=(a,b) \in \mathcal{K}$; $x, y \in Z_{26}$
    - $e_K(x) = (ax+b) \bmod 26$
    - $d_K(y) = a^{-1}(y-b) \bmod 26$

Introduction: Some Simple Cryptosystems

- e.g.: Suppose K=(7,3)
  - $7^{-1} \bmod 26 = 15$
  - Plaintext: student, Information
  - Ciphertext: ZGNYFQG

$e_K(x)=(7x+3) \bmod 26$

$d_K(y)=15(y-3) \bmod 26$

plaintext	s	t	u	d	e	n	t
	18	19	20	3	4	13	19
$e_K(x)$	25	6	13	24	5	16	6
ciphertext	Z	G	N	Y	F	Q	G

M1L3