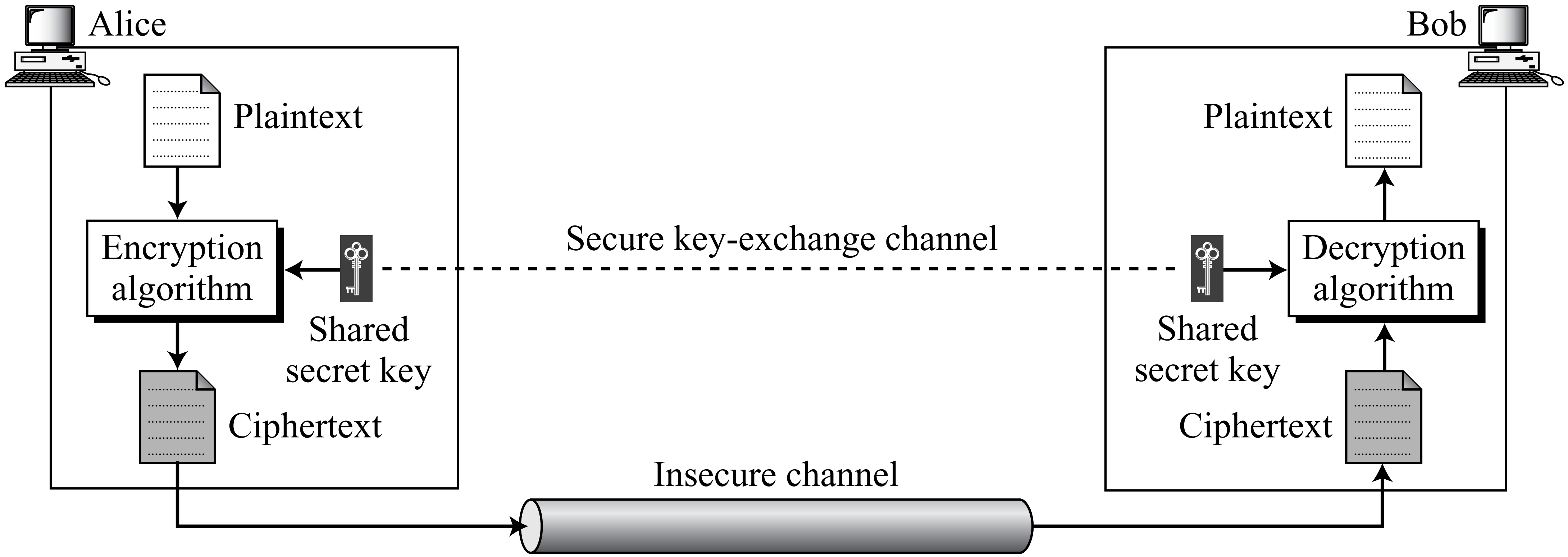
Symmetric Key Ciphers

Intro and Classification
Part I: Substitution Ciphers

Priyank Kalla
Professor
Electrical & Computer Engineering



- Ciphers: Encryption and Decryption Algorithms
- Plaintext P, Ciphertext C, key k, Encryption algorithm $E_k(P)$, Decryption algorithm $D_k(C)$
  - $C = E_k(P), \quad D_k(C) = P$
  - $D_k(E_k(x)) = E_k(D_k(x)) = x$: Encryption/Decryption are inverses of each other
- Need a "secure" key exchange mechanism — will study later
- **Symmetric**: same key for E_k, D_k and also for two-way communication between Alice $\Longleftrightarrow$Bob
- Need a separate key for each channel
- Key is the secret, E_k, D_k may be known to the public (adversary): Kerchoff's principle

Classification of Symmetric Key Ciphers (SKC)

- Traditional Ciphers versus Modern Ciphers (study later)
- Substitution Ciphers versus Transposition Ciphers
  - Substitution: Substitute one symbol with another
  - Transpose: Reorder the symbols
- Stream versus Block Ciphers
  - Stream: encipher/decipher one symbol (char or bit) at a time
  - $P = P_1P_2P_3, K = (k_1, k_2, k_3), C = C_1C_2C_3$
  - Block: encipher a block/group of plaintext symbols creating a block/group of ciphertext of the same size. Same key for the whole block.
    - $\{D, P, V\} = E_k(i, n, t)$

Examples

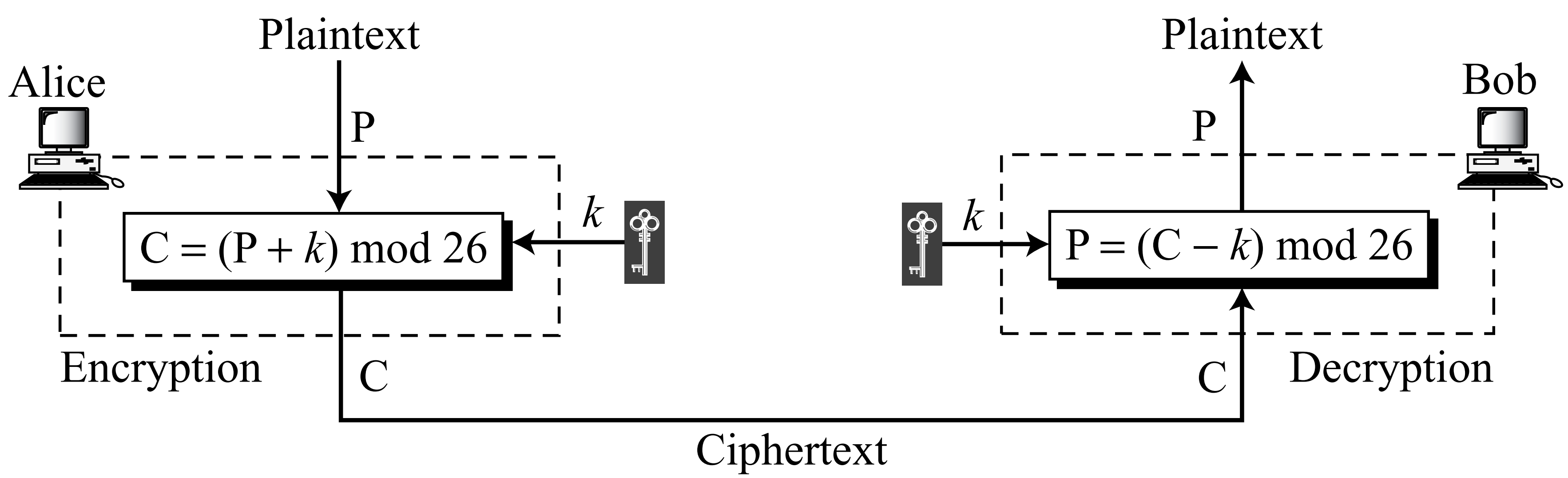
- Substitution ciphers:
  - Monoalphabetic: one-to-one correspondence between P and C. Ex: $P =$ hello, $C = KHOOR$
    - Examples: Additive Ciphers (Caeser cipher), Multiplicative Ciphers and Affine Ciphers (modulo n)
    - Not very secure today, susceptible to attacks
  - Polyalphabetic: each occurrence of a character may have a different substitute (one-to-many)
    - Ex: Vigenere cipher, Hill Cipher, Rotor Cipher, …
  - We'll study: Add/Mult and affine ciphers, and Hill Cipher
  - These are traditionally modulo arithmetic based $\pmod{n}$, often $n = 26$

Additive Cipher

Plaintext →	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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- P = consists of symbols (say, lower case)
- C = say, upper case symbols
- Assign an integer (modulo 26) to each symbol: arithmetic in $\mathbb{Z}_{26}$ — note this is NOT a finite field, but a ring!
- In $\mathbb{Z}_{26}$ every element has an additive inverse, but only some elements have multiplicative inverses
- Implications on key selection

Additive Cipher:



- Example $k = 15$

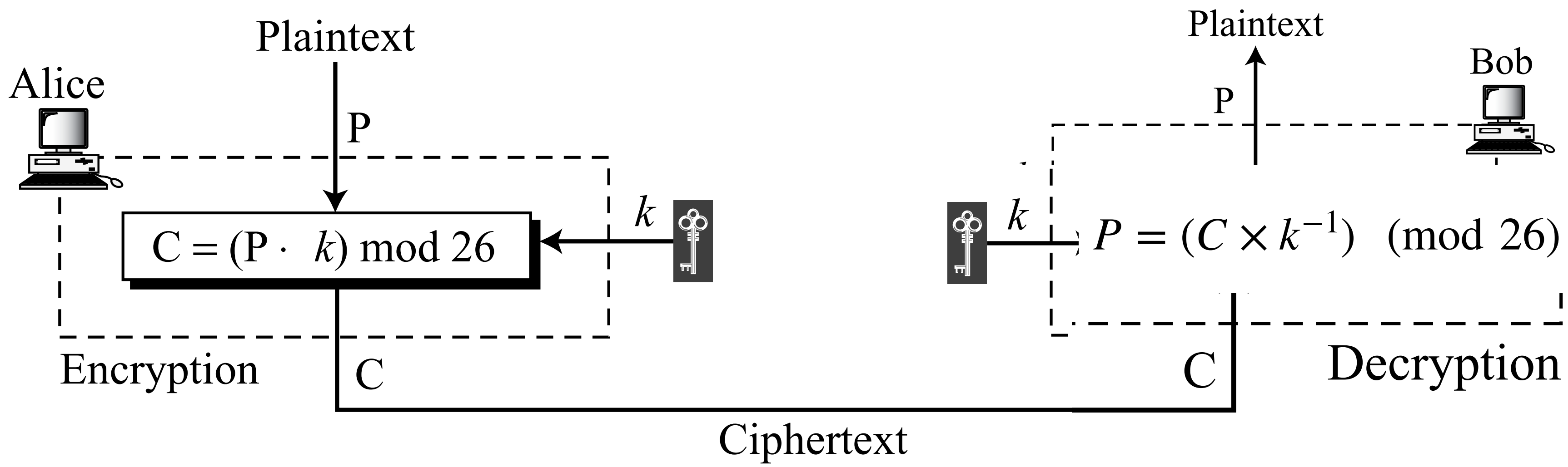
Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

Ciphertext: W → 22	Decryption: (22 − 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 − 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 − 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 − 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 − 15) mod 26	Plaintext: 14 → o

Julius Caesar used k = 3: Caeser cipher

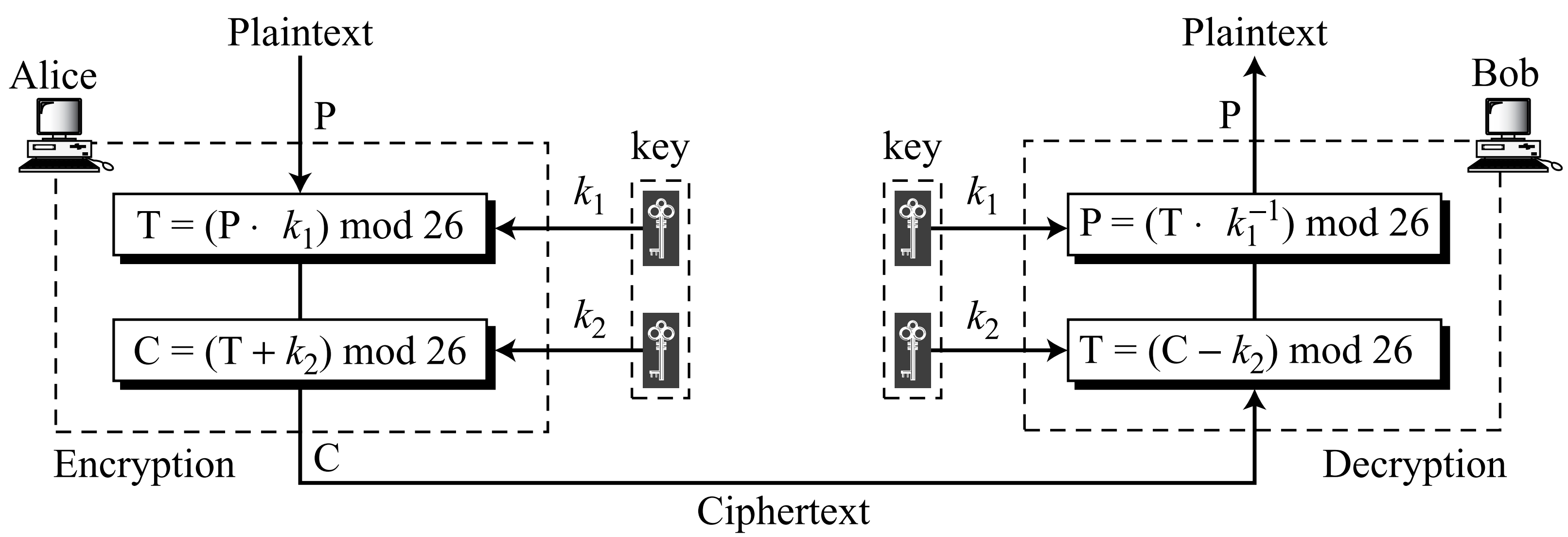
Additive Cipher susceptible to brute-force attacks key space = 25 (k = 0 is useless)

Multiplicative Cipher



- What can you say about the choice of k?
- Can only select those values of k s.t. multiplicative inverse exists
- $\mathbb{Z}_{26}{}^* = \{1,3,5,7,9,11,15,17,19,21,23,25\}$ = set of k for which $\exists k^{-1}$ s.t. $k \cdot k^{-1} = 1 \pmod{26}$
- Example: P = “e” = 4. $k = 7, k^{-1} = 15 \pmod{26}$
- $C = 4 \cdot 7 = 2 \pmod{26}$
- $P = 2 \cdot 7^{-1} = 2 \cdot 15 = 30 = 4 \pmod{26}$

Affine Cipher



$C = (P \times k_1 + k_2) \bmod 26$ $\qquad$ $P = ((C - k_2) \times k_1^{-1}) \bmod 26$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

- Let’s try an example of cryptanalysis using “chosen plaintext attack”
- Suppose Eve can access Alice’s cryptosystem, and create (P, C) pairs. Can she guess k_1, k_2?

Chosen Plaintext Attack Cryptanalysis

- Eve tries P = “et”, obtains C = “WF”

Plaintext: et	ciphertext: $\rightarrow$ WF

e $\rightarrow$ W	$04 \rightarrow 22$	$(04 \times k_1 + k_2) \equiv 22 \pmod{26}$
t $\rightarrow$ F	$19 \rightarrow 05$	$(19 \times k_1 + k_2) \equiv 05 \pmod{26}$

- Solve the system of Linear Congruences:

$$4k_1 + k_2 \equiv 22 \pmod{26}$$

- $$19k_1 + k_2 \equiv 05 \pmod{26}$$

- How to solve a system of Linear Congruences $\pmod{n}$?

- Need Matrix Algebra of residue classes $\pmod{n}$: Need matrix inversion algorithms $\pmod{n}$

- Solution: $k_1 = 11, k_2 = 4$

Linear Congruences

- $\begin{bmatrix} 4 & 1 \\ 19 & 1 \end{bmatrix} \cdot \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} 22 \\ 5 \end{bmatrix} \pmod{26}$
- $\begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 22 \\ 5 \end{bmatrix} \pmod{26}$
- Inverse of matrix A exists $\pmod{n}$ if det(A) has an inverse in $\mathbb{Z}_{26}$: GCD(det(A), n) = 1
- In our case above, det(A) = 4 -19 = 11 (mod 26).
- GCD(11, 26) = 1, so inverse exists
- Now how to compute Inverse of the matrix (mod n)? Next class!