CS 4173/5173
COMPUTER SECURITY

Some Early Ciphers

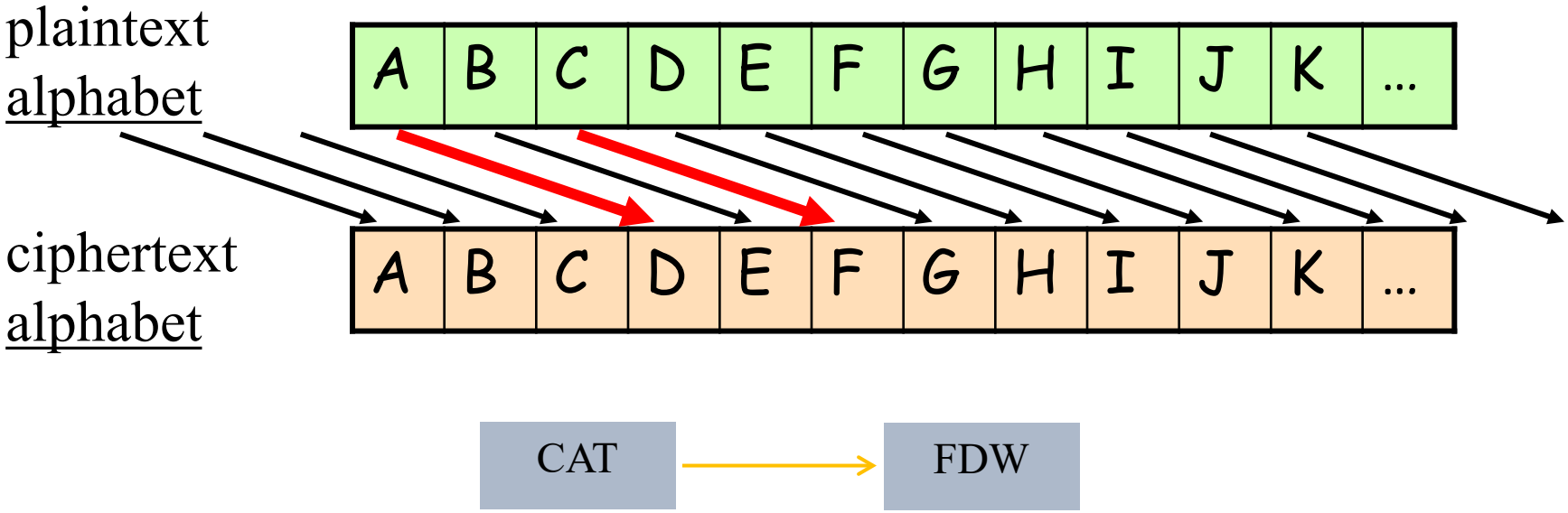
OUTLINE LAST TIME

- DoS/DDoS attack
  - Attack and defense strategies
- Cryptography vs Steganography
- Plaintext, ciphertext, encryption, decryption, key, cipher
- Three types of attack
  - Ciphertext only attacks
  - Known plaintext attacks
  - Chosen plaintext attacks

- Perfectly secure ciphers vs computationally secure ciphers

CAESAR CIPHER

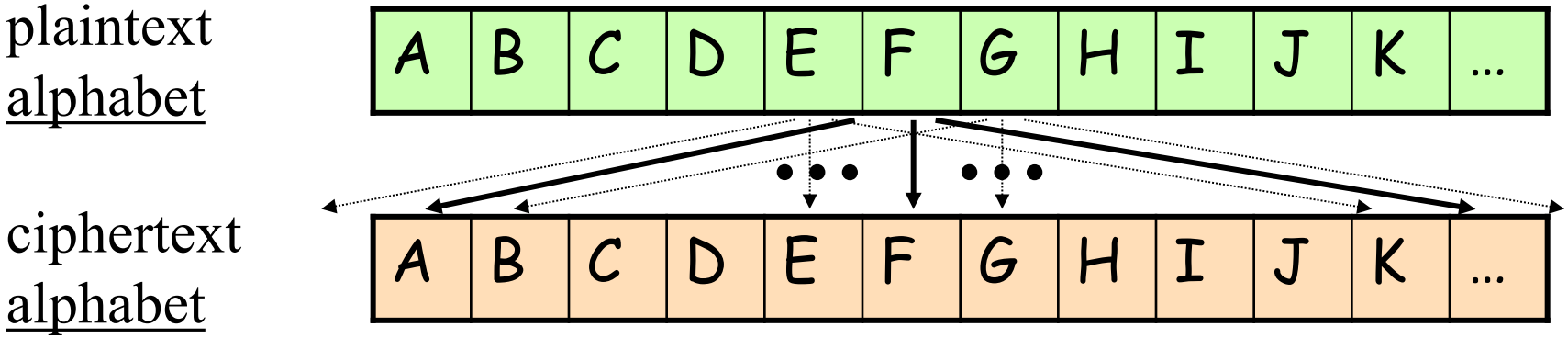
- Replace each letter with the one 3 letters later in the alphabet



Trivial to break

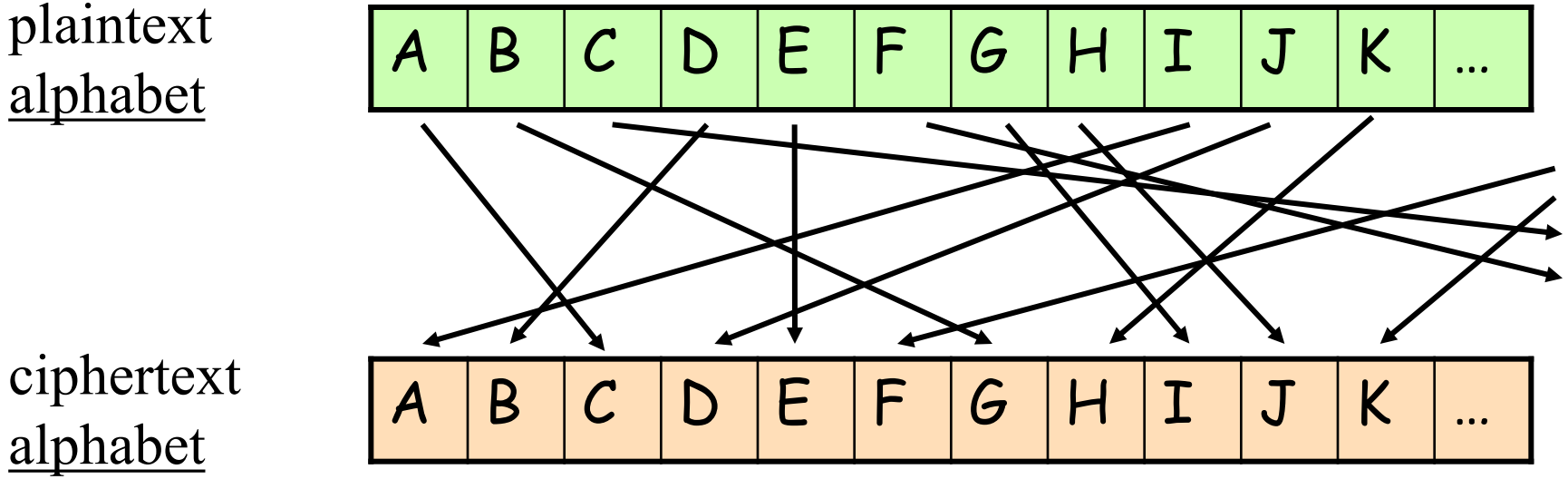
A VARIANT OF CAESAR CIPHER

- Replace each letter by one that is δ positions later, where δ is selectable (i.e., δ is the key)
  - example: IBM → HAL (for δ=25)
- Also, trivial to break with modern computers (how many possibilities?)



MONO-ALPHABETIC CIPHERS

- Generalized substitution cipher: randomly map one letter to another (How many possibilities?)
  - 26! ($\approx 2^{88}$)
- The key must specify which permutation; how many bits does that take?
  - log2(26!) ($\approx$ 88 bits)



ATTACKING MONO-ALPHABETIC CIPHERS

- Known plaintext attack
- Frequency of single letters in English language, taken from a large corpus of text:

A ≈ 8.2%	H ≈ 6.1%	O ≈ 7.5%	V ≈ 1.0%
B ≈ 1.5%	I ≈ 7.0%	P ≈ 1.9%	W ≈ 2.4%
C ≈ 2.8%	J ≈ 0.2%	Q ≈ 0.1%	X ≈ 0.2%
D ≈ 4.3%	K ≈ 0.8%	R ≈ 6.0%	Y ≈ 2.0%
E ≈ 12.7%	L ≈ 4.0%	S ≈ 6.3%	Z ≈ 0.1%
F ≈ 2.2%	M ≈ 2.4%	T ≈ 9.1%	
G ≈ 2.0%	N ≈ 6.7%	U ≈ 2.8%	

ATTACKING… (CONT'D)

- Suppose the attacker intercepts the following message

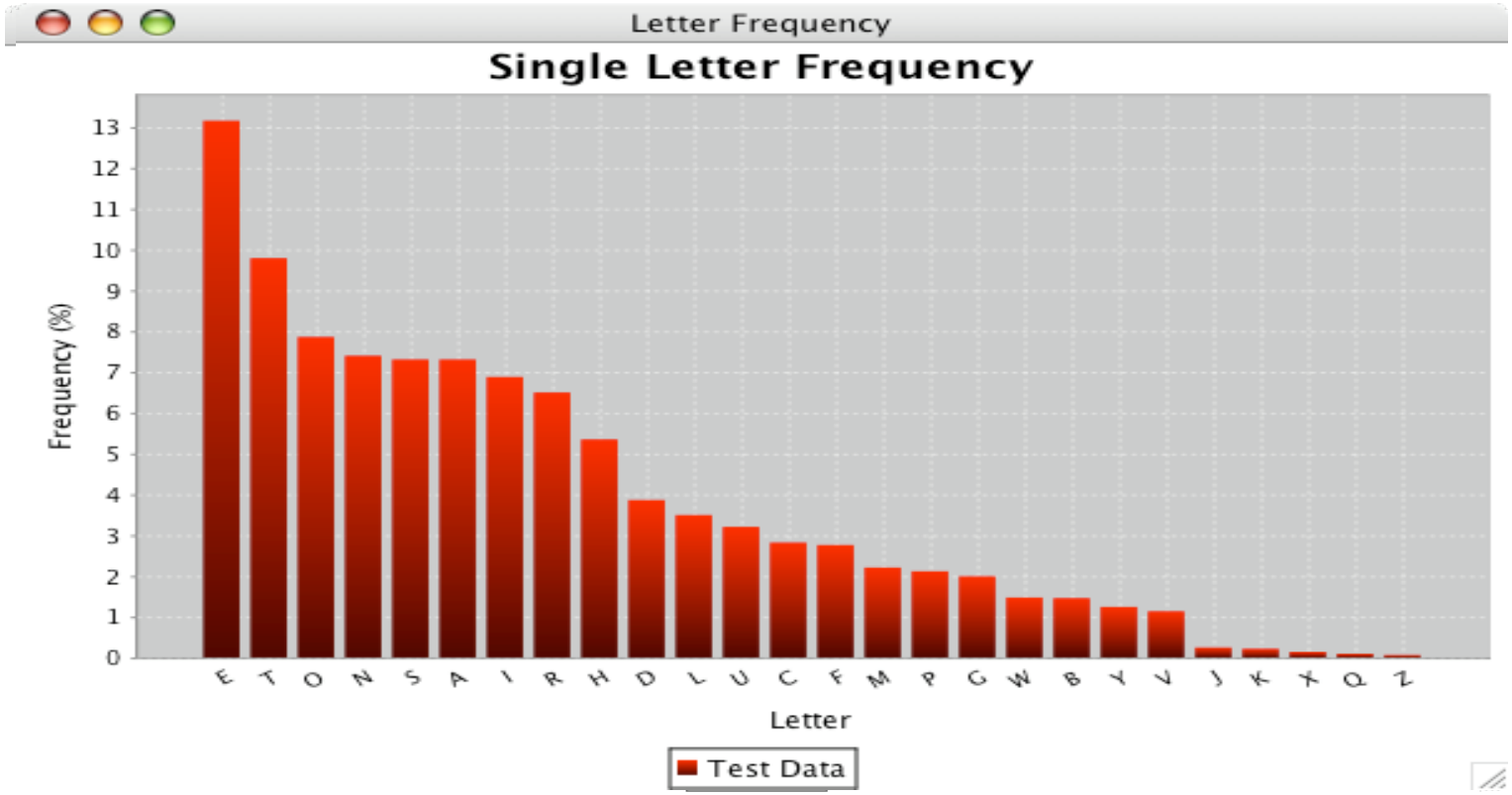
UXGPOGZCFJZJTFADADAJEJNDZMZHBBGZGGKQGVVGXCDIWGX

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
3	2	2	4	1	2	8	1	1	4	1	0	1	1	1	1	1	0	0	1	1	2	1	3	0	5

A ≈ 8.2%	H ≈ 6.1%	O ≈ 7.5%	V ≈ 1.0%
B ≈ 1.5%	I ≈ 7.0%	P ≈ 1.9%	W ≈ 2.4%
C ≈ 2.8%	J ≈ 0.2%	Q ≈ 0.1%	X ≈ 0.2%
D ≈ 4.3%	K ≈ 0.8%	R ≈ 6.0%	Y ≈ 2.0%
E ≈ 12.7%	L ≈ 4.0%	S ≈ 6.3%	Z ≈ 0.1%
F ≈ 2.2%	M ≈ 2.4%	T ≈ 9.1%	
G ≈ 2.0%	N ≈ 6.7%	U ≈ 2.8%	

FREQUENCY ANALYSIS IS AMAZING
NOW WE NEED BETTER CIPHER

LETTER FREQUENCIES



LETTER FREQUENCIES

LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVSTYLXZIXLIKIIXPIJVSZEYP
ERRGERIMWQLMGLMXQERIWGPSRIHMXQEREKIETXMJTPRGEVEKEITREWHEXXLEXXMZIT
WAWSQWXSWEXTVEPMRXRSJGSTVRIEYVIEXCVMUIMWERGMIWXMJMGCSMWXSJOMIQXL
IVIQIVIXQSVSTWHKPEGARCSXRWIEVSWIIBXVIZMXFSJXLIKEGAEWHEPSWYSWIWIEVXLISX
LIVXLIRGEPIRQIVIIBGIIHMWYPFLEVHEWHYPSRRFQMXLEPPXLIECCIEVEWGISJKTVWMRLI
HYSPHXLIQIMYLXSJXLIMWRIGXQEROIVFVIZEVAEKPIEWHXEAMWYEPPXLMWYRMWXSGS
WRMHIVEXMSWMGSTPHLEVHPFKPEZINTCMXIVJSVLMRSCMWMSWVIRCIGXMWYMX

I is the most common single letter
XL is most common bigram
XLI is the most common trigram

e is the most common single letter
th is most common bigram
the is the most common trigram

I => e
X => t
L => h

E is the second common single letter

E => a

LETTER FREQUENCIES

heVeTCSWPeYVaWHaVSReQMthaYVaOeaWHRtateFFaMVaWHKVSTYhtZetheKeetPeJVSZaYPa
RRGaReMWQhMGhMtQaReWGPSReHMtQaRaKeaTtMJTPRGaVaKaeTRaWHatthattMZeTWAWS
QWtSWatTVaPMRtRSJGSTVReaYVeatCVMUeMWaRGMeWtMJMGCSMWtSJOMeQtheVeQeVetQ
SVSTWHKPaGARCStRWeaVSWeeBtVeZMtFSJtheKaGAaWHaPSWYSWeWeaVtheStheVtheRGa
PeRQeVeeBGeeHMWYPFhaVHaWHYPSRRFQMthaPPtheaCCeaVaWGeSJKTVWMRheHYSPHth
eQeMYhtSJtheMWReGtQaROeVFVeZaVAaKPeaWHtaAMWYaPPthMWYRMWtSGSWRMHeVatM
SWMGSTPHhaVHPFKPaZeNTCMteVJSVhMRSCMWMSWVeRCeGtMWYMt

V => r

R => s

M => i
Z => m

LETTER FREQUENCIES

hereuponlegrandarosewithagraveandstatelyairandbroughtmethebeetlefromaglasscaseinwhichitwase
nclosedItwasabeautifulscarabaeusandatthattimeunknowntonaturalistsofcourseagreatprizeinascientifi
cpointofviewthereweretworoundblackspotsnearoneextremityofthebackandalongonenear theotherthes
caleswereexceedinglyhardandglossywithalltheappearanceofburnishedgoldtheweightoftheinsectwasv
eryremarkableandtakingallthingsintoconsiderationicouldhardlyblamejupiterforhisopinionrespectingit

Hereupon Legrand arose, with a grave and stately air, and brought me the beetle from a glass case in which it was enclosed. It was a beautiful scarabaeus, and, at that time, unknown to naturalists—of course a great prize in a scientific point of view. There were two round black spots near one extremity of the back, and a long one near the other. The scales were exceedingly hard and glossy, with all the appearance of burnished gold. The weight of the insect was very remarkable, and, taking all things into consideration, I could hardly blame Jupiter for his opinion respecting it.

Frequency Analysis: https://en.wikipedia.org/wiki/Frequency_analysis

VIGENERE CIPHER

- A set of mono-alphabetic substitution rules (shift amounts) is used
  - the key determines what the sequence of rules is
  - also called a *poly-alphabetic* cipher

- Ex.: key = (3 1 5)
  - i.e., substitute first letter in plaintext by letter+3, second letter by letter+1, third letter by letter+5
  - then repeat this cycle for each 3 letters

VIGENERE… (CONT'D)

- Ex.: plaintext = "BANDBAD"

plaintext message

B	A	N	D	B	A	D

shift amount

3	1	5	3	1	5	3

ciphertext message

E	B	S	G	C	F	G

What are the possible attacks?

- Frequency analysis?

HISTORY

- First developed 1553
- easy to understand, but resisted all attempts to break it for three centuries
- A general method to crack 1863

HILL CIPHERS

- Encrypts *m* letters of plaintext at each step
  - i.e., plaintext is processed in blocks of size *m*

- Encryption of plaintext p to produce ciphertext c is accomplished by: $c = \boldsymbol{K}p$
  - the $m \times m$ matrix $\boldsymbol{K}$ is the key
  - decryption is multiplication by inverse: $p = \boldsymbol{K}^{-1}c$
  - *remember: all arithmetic mod 26*

HILL CIPHER EXAMPLE

- For $m = 2$, let $\boldsymbol{K} = \begin{matrix} 1 & 2 \\ 3 & 5 \end{matrix}$, $\boldsymbol{K}^{-1} = \begin{matrix} 21 & 2 \\ 3 & 25 \end{matrix}$

Plaintext p =

A	B	X	Y	D	G
0	1	23	24	3	6

$$c = Kp = \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

(21*15+2*13) mod 26

=(1*0+2*1) mod 26

(3*23+5*24) mod 26

Ciphertext c =

2	5	19	7	15	13
C	F	T	H	P	N

PERMUTATION CIPHERS

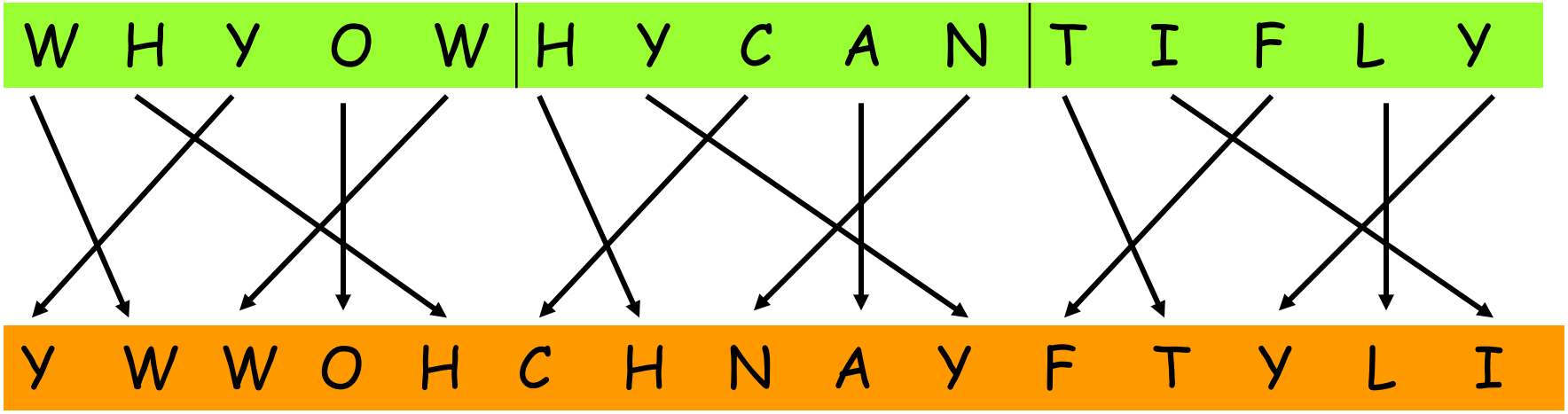
- The previous codes are all based on substituting one symbol in the alphabet for another symbol in the alphabet

- Permutation cipher: permute (rearrange, transpose) the letters in the message
  - the permutation can be fixed, or can change over the length of the message

PERMUTATION… (CONT'D)

- Permutation cipher ex. #1:
  - Permute each successive block of 5 letters in the message according to position offset <+1,+3,-2,0,-2>

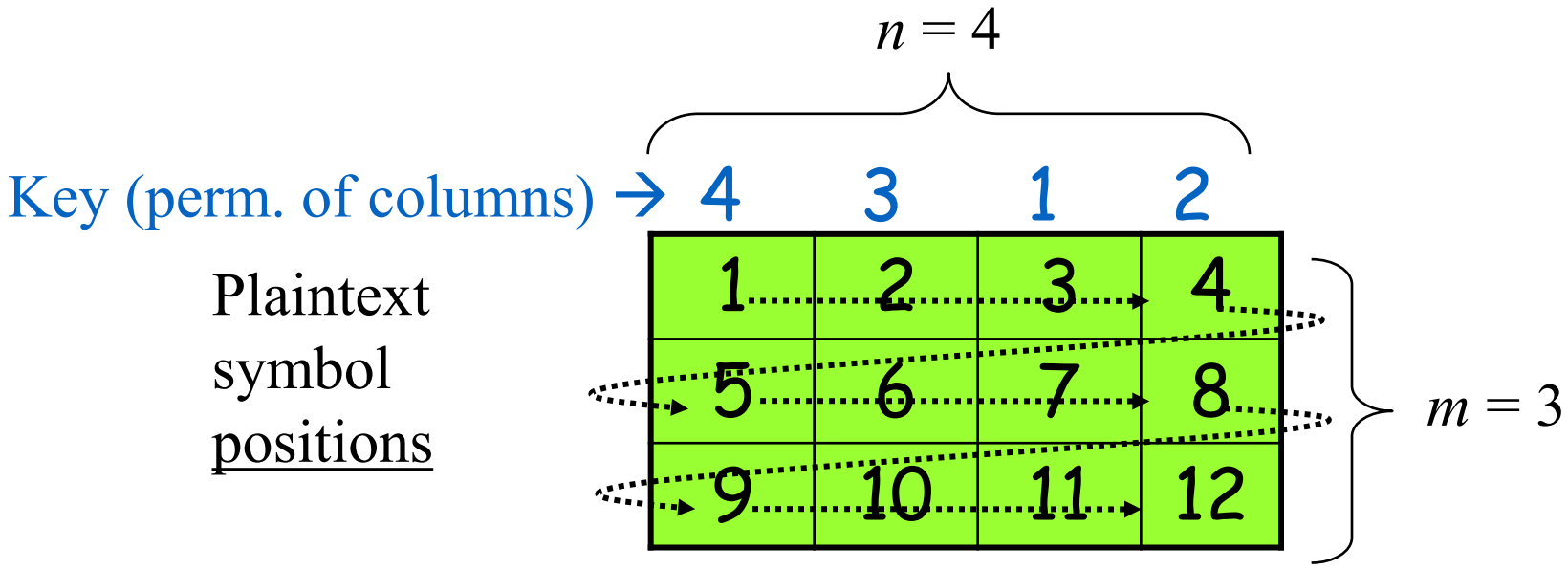
plaintext message



ciphertext message

PERMUTATION… (CONT'D)

- Permutation cipher ex. #2:
- arrange plaintext in blocks of n columns and m rows
- then permute columns in a block according to a key K

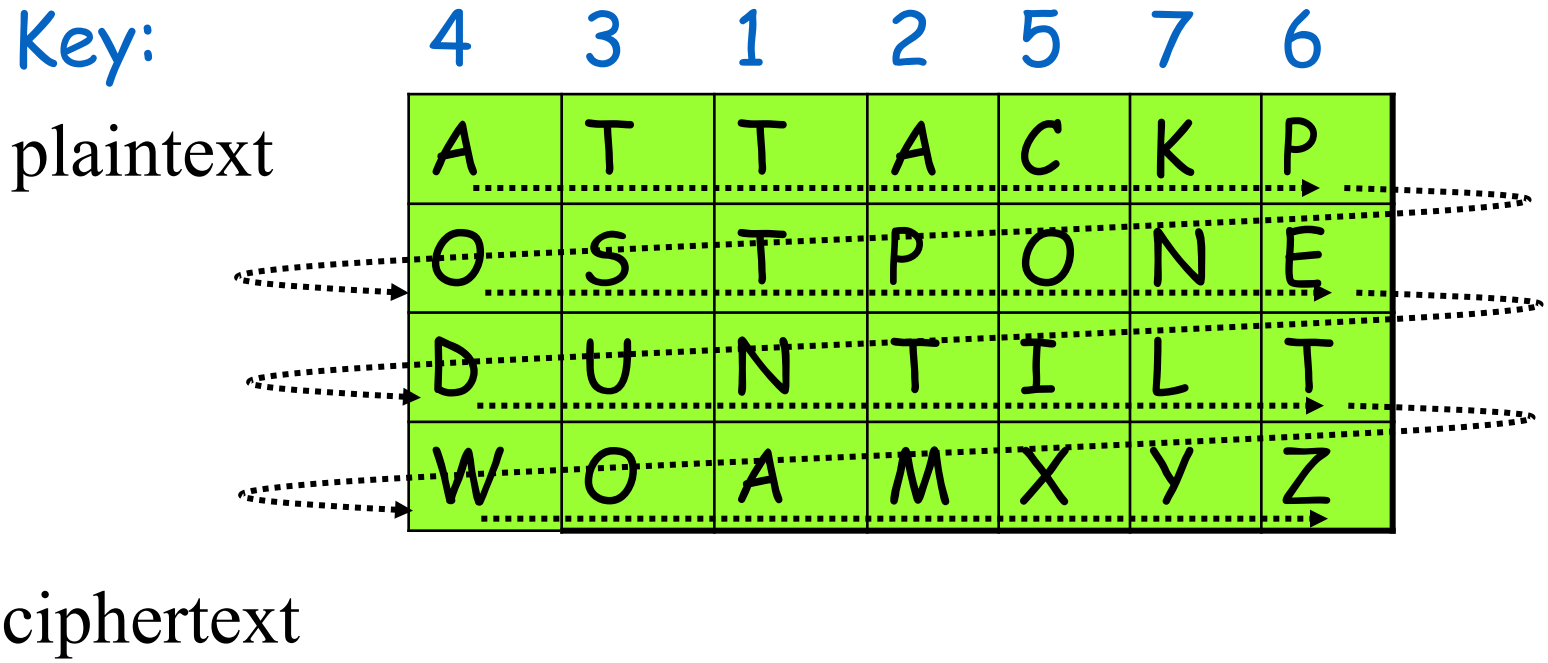


ciphertext sequence (by plaintext position) for one block

3	7	11	4	8	12	2	6	10	1	5	9

PERMUTATION… (CONT'D)

- A longer example: plaintext = "ATTACK POSTPONED UNTIL TWO AM"



TTNA APTM TSUO AODW COIX PETZ KNLY

PERFECTLY SECURE CIPHERS

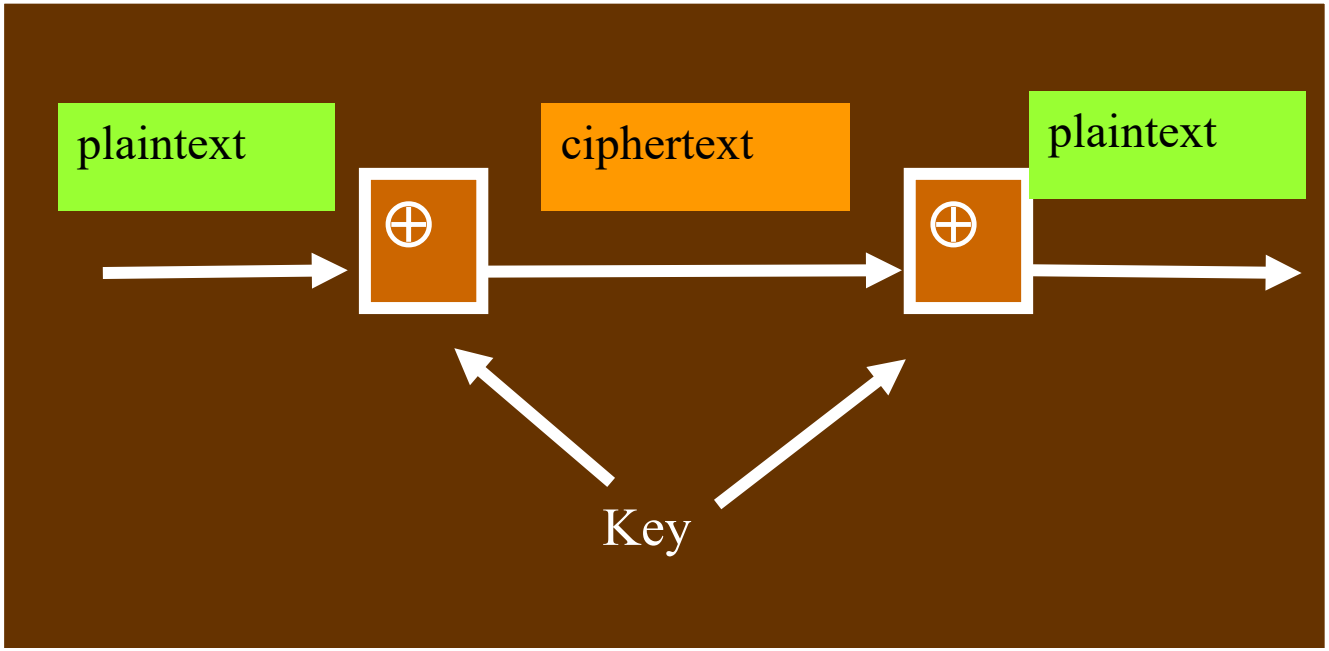
1. Ciphertext does not reveal any information about which plaintexts are more likely to have produced it
   – e.g., the cipher is robust against ciphertext only attacks

and

2. Plaintext does not reveal any information about which ciphertexts are more likely to be produced
   – e.g, the cipher is robust against known/chosen plaintext attacks

ONE-TIME PAD (OTP)

- Idea
  - generate a random bit string (the key) as long as the plaintext, and share with the other communicating party
  - encryption: XOR this key with plaintext to get ciphertext
  - decrypt: XOR same key with ciphertext to get plaintext

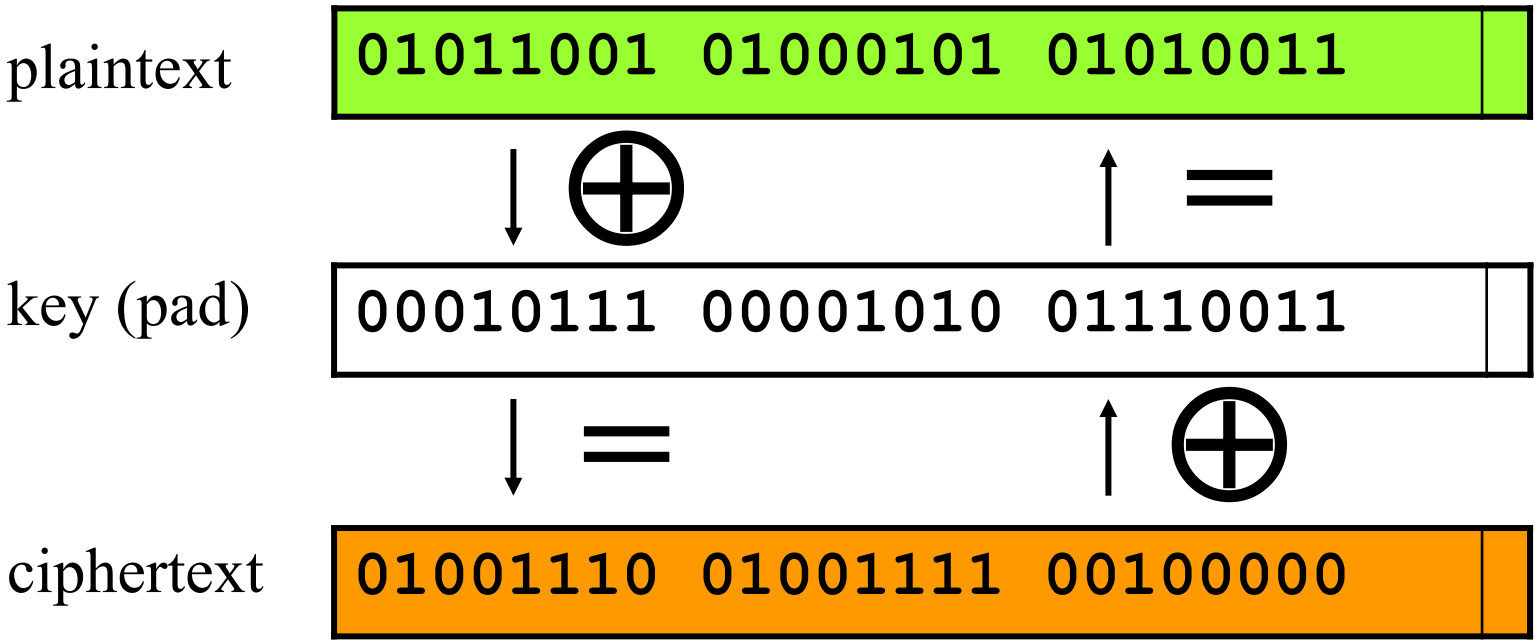


XOR

- For bits a, b
  - a XOR b = (a + b) mod 2

- 0 XOR 0 = 0
- 1 XOR 0 = 1
- 0 XOR 1 = 1
- 1 XOR 1 = 0

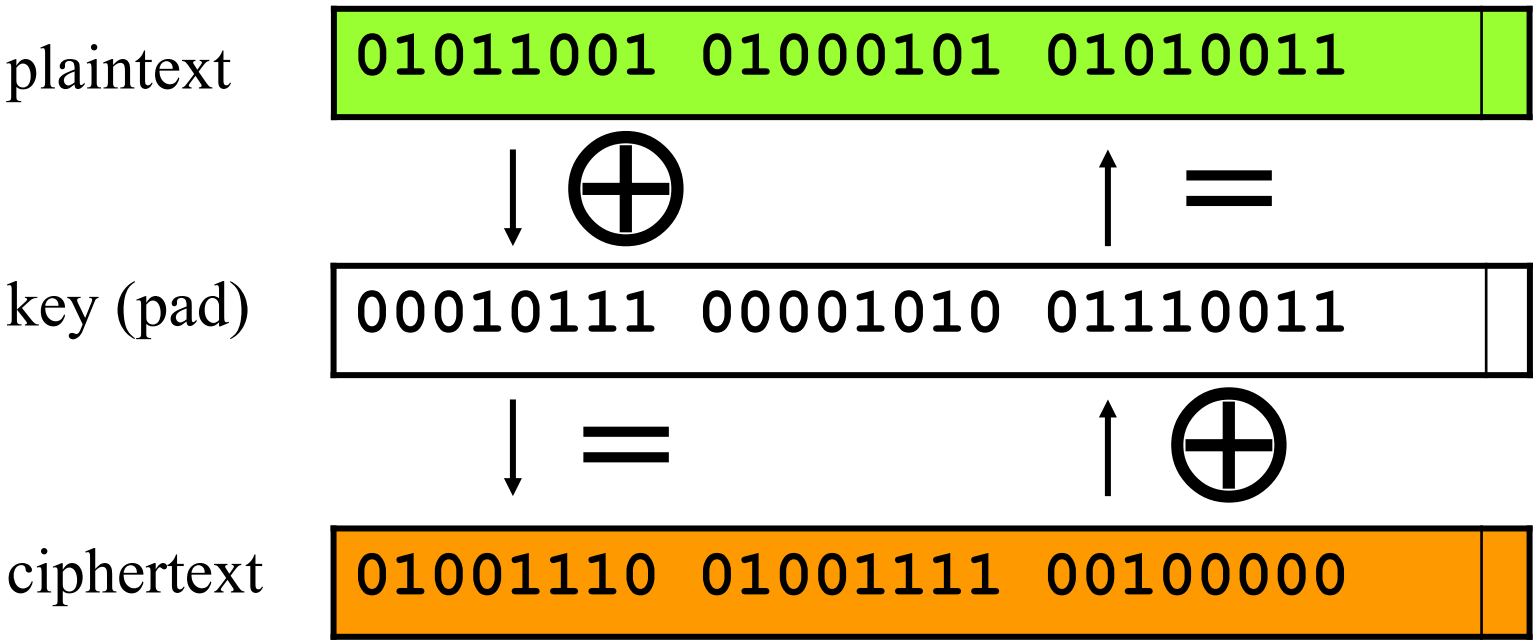
OTP… (CONT'D)



- Why can't the key be reused?
- Is this secure?

OTP SECURITY

- OTP is proven to be **perfectly secure**!
  - We will get it next lecture. Get ready for some probability stuff
- Try to explain in an intuitive way.



CIPHER SUMMARY

- Easy thing:
  - design a cipher that maps a plaintext into a random-looking ciphertext.

- Hard things:
  - hard to develop an attack.
  - hard to prove the cipher is secure against all possible attacks

CS 4173/5173
COMPUTER SECURITY

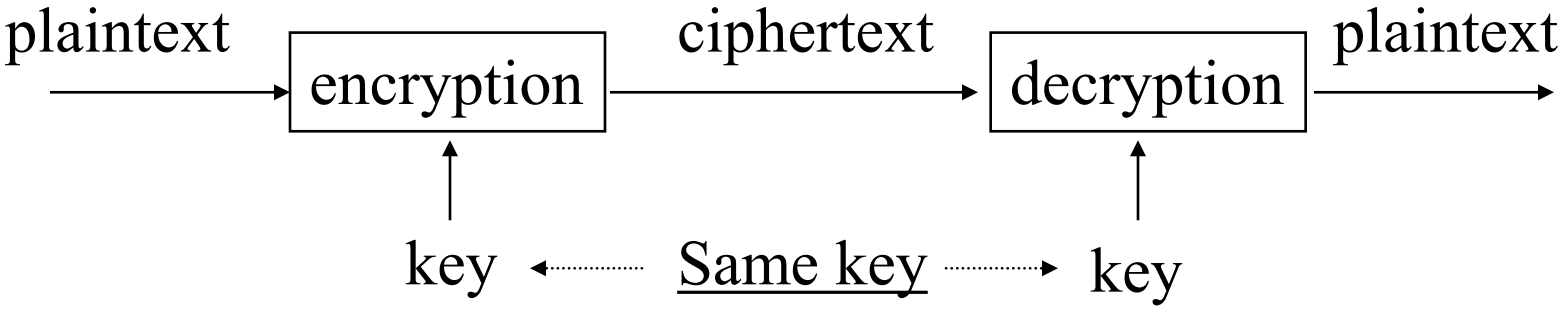
Some "Key" Issues
Typical Ciphers Today

TYPES OF CRYPTOGRAPHY

- Number of keys
  - Secret key cryptography: one key
  - Public key cryptography: two keys
  - Hash functions: no key

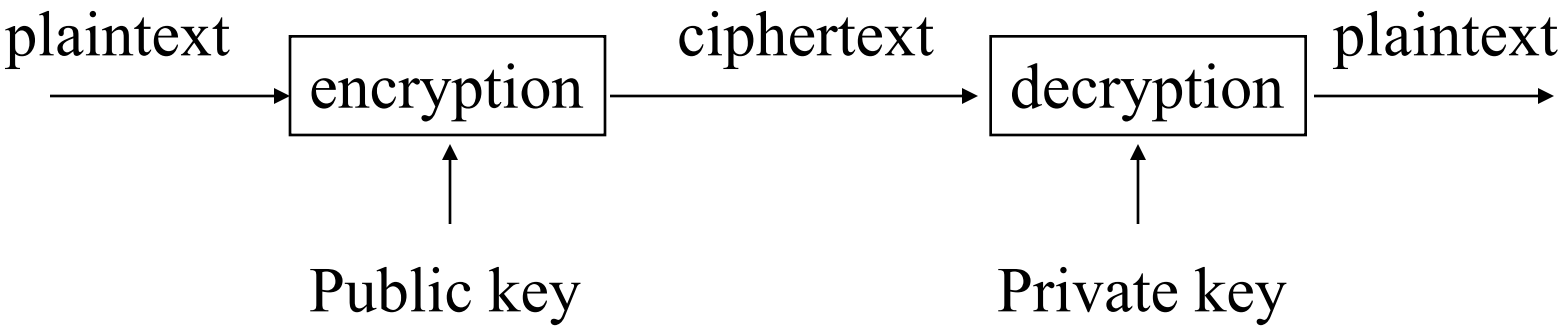
- The way in which the plaintext is processed
  - Stream cipher: encrypt input message one symbol at a time
  - Block cipher: divide input message into blocks of symbols, and processes the blocks in sequence
    - May require padding

SECRET KEY CRYPTOGRAPHY



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

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

HASH ALGORITHMS

- Also known as
  - Message digests
  - One-way transformations
  - One-way functions
  - Hash functions
- Length of $H(m)$ much shorter than length of m
- Usually fixed lengths: 128, 160, 256, 512 bits

SUMMARY

- Early ciphers aren't nearly strong enough
  - Still need some efforts to crack.
- Key issues
  - Secret key cryptography
  - Public key cryptography
  - Hash

WEAK LINK IN SECURITY

- Cryptography is a fundamental, and most carefully studied, component of security
  - Modern ciphers are based on computational difficulty.
  - Not usually the “weak link”.
  - Today, human beings are often considered the “weakest link” in a security system