Last Time

- Computer and network security: protection of hardware, software, and data of computer systems
- Security goals: confidentiality, integrity, and availability
- An adversary exploits a vulnerability to launch an attack
- Security model: trust model + threat model

Intuition

- Cryptography is the art (and sometimes science) of secret writing
  - Come from the Greek words κρυπτο (*hidden or secret*) and γραφη (*writing*)
- Traditionally used to prevent others from reading the information sent between participants
- Less well known that it is also used to guarantee other properties, e.g., integrity of data

Cryptosystem

- A cryptosystem is a 5-tuple (*E*, *D*, *M*, *K*, *C*)
  - *E*: encryption algorithm
  - *D*: decryption algorithm
  - *M*: the set of plaintext
  - *K*: the set of keys
  - *C*: the set of ciphertext

Cryptosystem

- Plaintext: a message in its original form
- Ciphertext: the mangled (i.e., encrypted) message
- Key: an input to a cryptographic algorithm
  - Security of the cryptosystem often depends on keeping the key secret
- Encryption algorithm: algorithm used to make messages unreadable by all but the intended receivers
  - *E(plaintext, key) = ciphertext*, i.e., $E(m, k_e) = c$
- Decryption algorithm: the reverse of encryption algorithm
  - *D(ciphertext, key) = plaintext*, i.e., $D(c, k_d) = m$

Hardness and Security

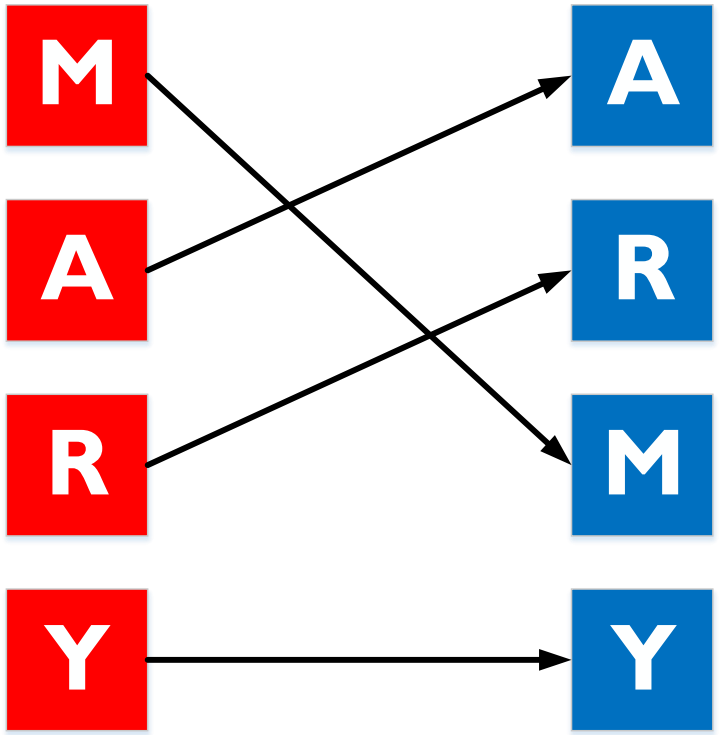
- Algorithm is public, key is private (Why?)
- A good cryptographic algorithm
  - Computing *c* from m with k_e and computing m from *c* with k_d are computationally easy
  - Computing m from *c* without k_d is computationally difficult

Secret Key Cryptography

- Symmetric keys, where a single key is used for both encryption and decryption algorithms
  - $E(m, k) = c$ and $D(c, k) = m$
- Management of keys determines who has access to encrypted data
- Also known as symmetric key cryptography

Transposition Cipher

- Permute the symbols in plaintext to produce ciphertext



- Question: What is the plaintext? What is the ciphertext? Is there a key?

Example: Rail Fence Cipher

- Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows

Plaintext M E E T M E A F T E R T H E T O G A P A R T Y

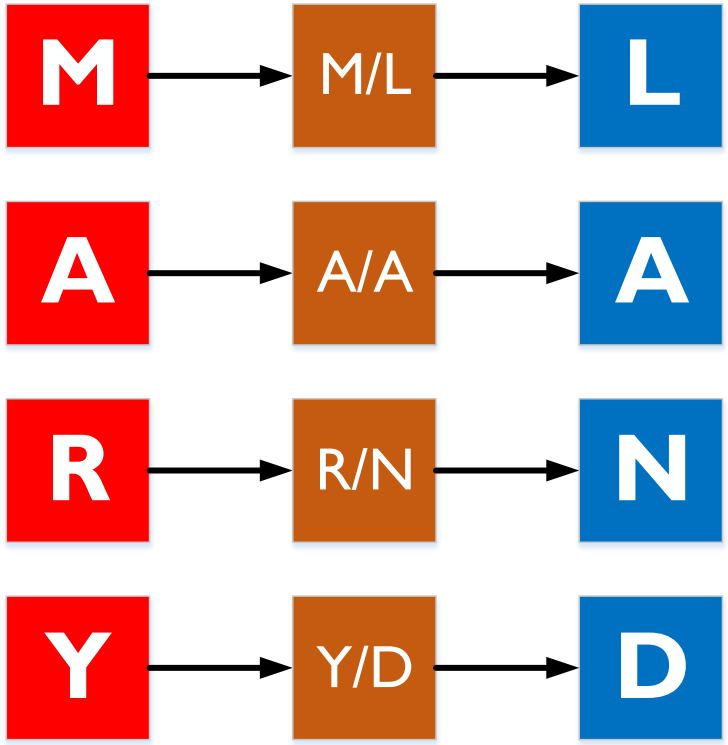
M E M A T R H T G P R Y

E T E F E T E O A A T

Ciphertext M E M A T R H T G P R Y E T E F E T E O A A T

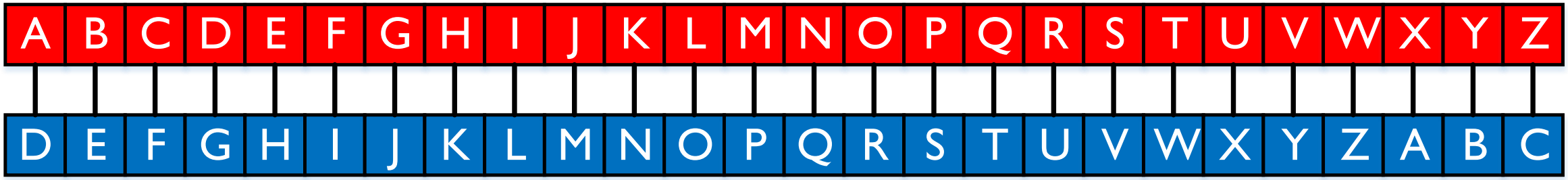
Substitution Cipher

- Substitutes one symbol for another



- Question: What is the key?

Example: Caesar Cipher

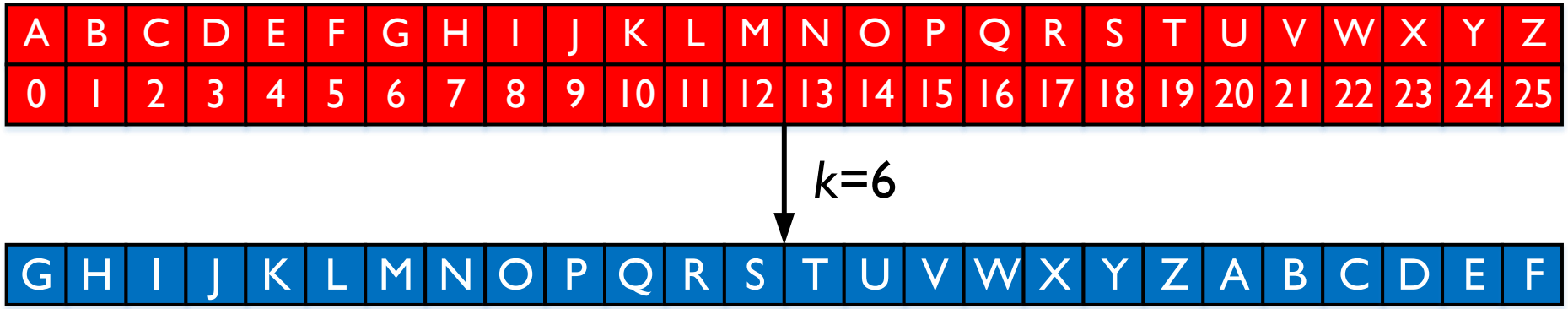


- Each letter in the alphabet is replaced with the letter three slots to the right

Plaintext	S	E	C	U	R	I	T	Y	A	N	D	P	R	I	V	A	C	Y							
Ciphertext	V	H	F	X	U	L	W	B	D	Q	G	S	U	L	Y	D	F	B							

Example: Caesar Cipher

- Generalization of Caesar cipher
  - Index the letters in alphabet from 0 to 25. Each ciphertext letter $c = E(m, k) = (m+k) \bmod 26$, where k takes the value in [1, 25]



- Question: what is the key?

S E C U R I T Y A N D P R I V A C Y

A M K C Z Q B G I V L X Z Q D I K G

Attack

- Brute-force attack
  - Attacker tries every possible key on a ciphertext until an intelligible translation into plaintext is obtained.
  - In the worst case, the attacker has to try all possible keys
  - On average, half of all possible keys must be tried

- Launch Brute-force attack on the following ciphertext

Z C F M V J V T L I Z K P

Example: One-Time Pad

- Is there an unbreakable cipher?
- One-Time Pad
  - Use a random bit string (also called a pad) as the key, which is with the same length as the plaintext
  - Encrypt the plaintext by XOR it with the random bit string; decrypt the ciphertext by XOR it with the random bit string

    $c = E(m, k) = m \text{ XOR } k; m = D(c, k) = c \text{ XOR } k$
  - The random bit string is used to encrypt and decrypt only one message, and then it is discarded
  - Perfectly secure: assume the value of each bit in k is equally likely, then you have no information to work with
  - Why is one-time pad not commonly used in practice?