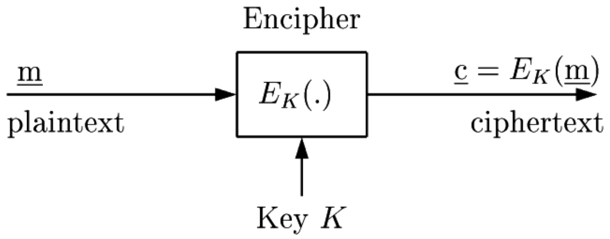
Introduction to Cryptography

ECEN 1200,
Telecommunications 1

Secret Writing

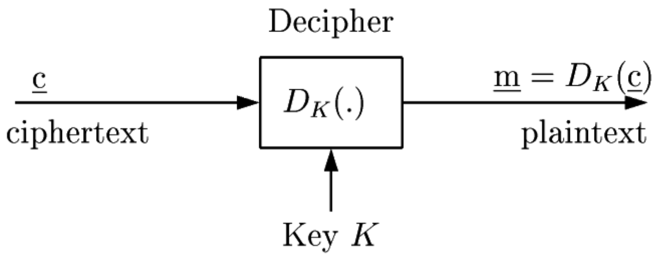
- **Cryptography** is the science and study of secret writing.
- More specifically, cryptography is concerned with techniques for enciphering data under control of a secret key K.
- A cryptographic algorithm or **cipher** is a pair of mathematical functions E_K, D_K, used for encryption and decryption.

Encryption



- The plaintext message m is encrypted using the secret key K and the encryption function $E_K(.)$, resulting in the ciphertext c.
- Example: m = hello => c = khoor

Decryption



- To recover the plaintext m, the ciphertext c is decrypted using the secret key K and the decryption function $D_K(.)$.
- Example: c = khoor => m = hello

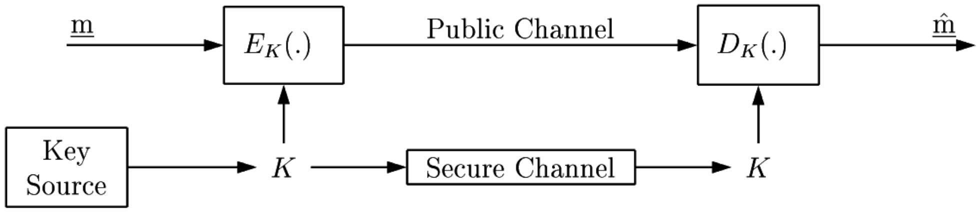
Security of Cryptographic System

- If the security of a cryptographic algorithm is based on keeping the algorithm secret, it is called a **restricted** algorithm.
- Modern cryptography assumes that the encryption and decryption functions are **publicly** known and analyzed.
- In this case all of the security is based in the secret encryption/decryption keys.

Kerckhoffs's (1835-1903) Principle

- The strength of a cryptographic system cannot be based on the secrecy of the system itself, because sooner or later someone will reverse-engineer the system.
- In fact, the workings of a cryptographic algorithm should be publicized as widely as possible so that weaknesses become known.
- Security has to rest entirely with the secret key.

Communication Using Classical Cryptography

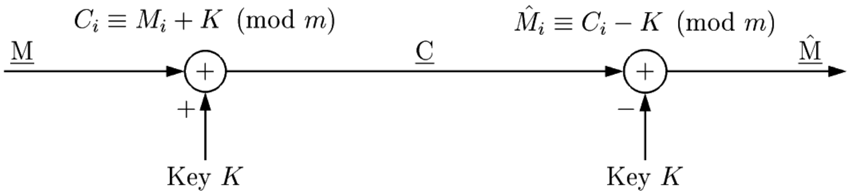


- The (fast) public channel (e.g., Internet) over which encrypted message is sent is insecure.
- The secret key K is distributed over a (slow) secure channel (e.g., using a courier).

Classical Ciphers

- There are two basic types of ciphers: Transpositions and substitutions.
- **Transposition ciphers** rearrange bits or characters in the data, e.g., using some geometric pattern.
- **Substitution ciphers** replace bits, characters, or blocks of data by substitutes, e.g., letters are replaced by different letters in the alphabet.

Caesar Cipher


$C_i \equiv M_i + K \pmod{m}$
$\hat{M}_i \equiv C_i - K \pmod{m}$
M
C
$\hat{\text{M}}$
+
+
+
−
Key K
Key K

- Using the numbers below, plaintext is converted to ciphertext by adding K modulo m=26.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Modulo *m* Arithmetic

- Given a positive integer m, the integer x can be expressed as

  x = q*m + r , 0 <= r < m .

- The integer q is the quotient
- The integer r is the remainder, also expressed as:

$$r = R_m(x)\,, \qquad \text{“}r \text{ is remainder of } x \text{ when divided by } m\text{”}\,,$$

$$r \equiv x \pmod{m}\,, \qquad \text{“}r \text{ is congruent to } x \text{ modulo } m\text{”}\,.$$

Addition modulo *m*=5, *m*=6

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

m=5

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

m=6

Multiplication modulo *m*=5, *m*=6

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

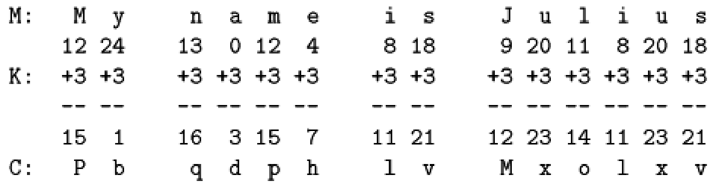
m=5

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

m=6

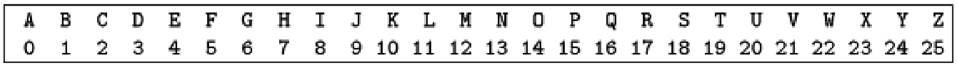
Example: Caesar Cipher, K=3

- The plaintext “My name is Julius” could be encrypted as follows using K=3:



```
M:   M  y     n  a  m  e     i  s     J  u  l  i  u  s
    12 24    13  0 12  4     8 18     9 20 11  8 20 18
K:  +3 +3    +3 +3 +3 +3    +3 +3    +3 +3 +3 +3 +3 +3
    -- --    -- -- -- --    -- --    -- -- -- -- -- --
    15  1    16  3 15  7    11 21    12 23 14 11 23 21
C:   P  b     q  d  p  h     l  v     M  x  o  l  x  v
```

- The ciphertext is “Pb qdph lv Mxolxv” if spaces and upper/lowercase letters are replicated



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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Convention Used for Plain/Cipher Texts in Classical Cryptography

- Keeping spaces between words and capitalization in the ciphertext gives away too many clues.
- Thus, plaintexts and ciphertexts are typically written in groups of 5 using all uppercase, e.g,

plain: `MYNAM EISJU LIUS`

cipher: `PBQDP HLVMX OLXV`

Keyspace

- The **keyspace** of a cipher is the total number of different keys that are possible.
- For the Caesar cipher with modulus m=26, a total of 26 different keys K are possible.
- Since the security of a cryptographic system is based on the secret key, a **large keyspace** (much larger than 26) is necessary, especially in connection with computers.

Simple Substitution Cipher

- Rather than just shifting the alphabet, an arbitrary substitution of a cipher letter for each plain letter can be made, e.g.,

plain:	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
cipher:	S	L	G	C	Z	V	K	R	N	B	Q	H	O	E	X	M	Y	P	W	D	A	J	U	I	R	T

- Using this, SUNSHINE would be encrypted as

  plain: S U N S H I N E
  cipher: W A E W R N E Z

Vigenère Cipher

- A Vigenère cipher consists of several shift (or Caesar) ciphers with different keys $k_1,k_2,..,k_L$ that are applied to the plaintext periodically.
- Example: Using keyword STAR and 26 letter alphabet (0…25)

```
  plain:  EAVESDROPPER
    key:  STARSTARSTAR
 cipher:  WTVVKWRFHIEI
```

Transposition Ciphers

- For a transposition cipher the unchanged plaintext letters are rearranged, e.g., using a rectangular array where the plaintext is read in as rows and the ciphertext is read out as columns.

Transposition Cipher Example

- Plaintext: MOVEF ORWAR DASAG REEDX (note the X to obtain the required length)
- Fill rectangular 4x5 array row-wise

```
MOVEF
ORWAR
DASAG
REEDX
```

- Ciphertext: MODRO RAEVW SEEAA DFRGX (read out column-wise left to right)

Keys, Keyspace

- Since the security of a cryptosystem depends on the secrecy of the (decryption) key, it is important that the number of possible keys is large enough to make an exhaustive search of all possible keys infeasible.
- The set of all possible keys for a given cryptosystem is called the keyspace and the number of all keys is the size of the keyspace.

Size of Keyspace

- Casear cipher: 26
- Simple substitution: 26! = $4x10^{26}$
- Arbitrary transposition on 40 letters: 40! = $8x10^{47}$

Exhaustive Search

- 1 day has 24*3600 = 86,400 sec
- 1 year has 365.25*86,400 = 31,557,600 sec
- 100 years has approx $3x10^{9}$ sec
- At 1 GHz, single computer can do $3x10^{18}$ operations in 100 years
- ➔ Arbitrary transposition on 40 letters takes approx $0.5*8*10^{47}/(3*10^{18}) = 1.3*10^{29}$ computers 100 years to solve!

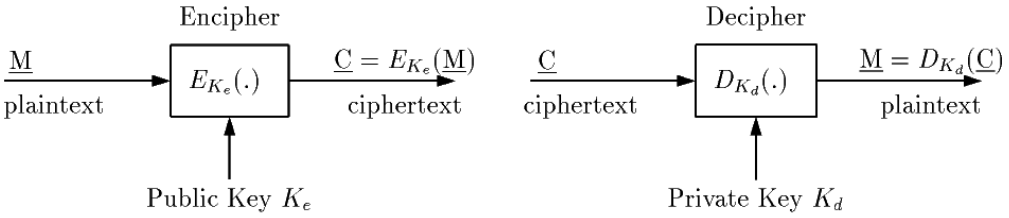
Key Distribution

- Suppose there are N users in a system and each possible pair of users has to be able to communicate securely with each other.
- That requires N(N-1)/2 secret key pairs that need to be distributed over secure channels.
- If N=1,000,000 then almost 500,000,000,000 key pairs are needed => **logistics nightmare!**

Public-Key Cryptography

- The key distribution problem can be solved elegantly if the encryption key K_e can be made public and only the decryption key K_d is secret.
- Clearly K_e and K_d must be related so that messages can be encrypted and decrypted without ambiguity.
- It should be easy to derive K_e from K_d. But it must be **very difficult** to obtain K_d from K_e.

Public-Key Cryptography



This works if
Easy: K_d => K_e
Difficult: K_e => K_d

One-Way Functions

- A function *f(.)* such that *y=f(x)* is easy to compute but *x=f*$^{-1}$*(y)* is very difficult to compute.
- Factorization: Given two large primes *p,q* it is easy to compute *m=p*q*. But given only *m*, it is very hard to find *p* and *q*.
- Discrete Logarithm Problem: Given *x* and *n* it is easy to compute *y=x*^{n} *(mod m)*. But computing *n=logx(y) (mod m)* is very hard.

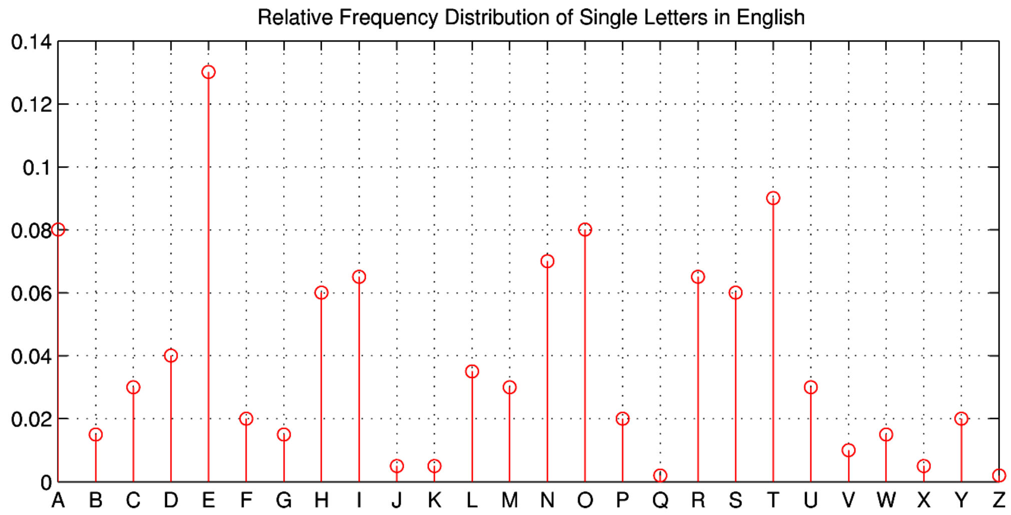
Cryptanalysis

- Three main types of attacks are:
  - Ciphertext-only attack
  - Known-plaintext attack
  - Chosen-plaintext attack

Ciphertext-only Attack

- Cryptanalyst has ciphertext of several messages, all of which have been encrypted using the same algorithm.
- Cryptanalyst tries to recover as much plaintext as possible or, better yet, to deduce the secret key.

Single Letter Frequency in English



Known-plaintext Attack

- Cryptanalyst has several plaintext-ciphertext pairs.
- Cryptanalyst tries to deduce the key used for enciphering/deciphering so that other messages encrypted with the same key can be deciphered.

Chosen-plaintext Attack

- Cryptanalyst can choose several plaintexts and obtain the corresponding ciphertexts.
- Cryptanalyst tries to deduce the key used for enciphering/deciphering so that other messages encrypted with the same key can be deciphered.
- Note: Chosen-plaintext attack is the main scenario for public-key cryptosystems.

Block Cipher

- To better conceal the statistical properties of the plaintext, blocks of letters or bits (e.g., 128 or 256 bits, corresponding to 16 or 32 characters) can be enciphered simultaneously.

Stream Cipher

- Another approach is generate a running key-stream and add it modulo m to the ciphertext.
- This is similar to the idea of the Vigenère cipher, except that the period (if any) is made very long.
- Note: Adding two plaintexts together is not good enough, the key-stream needs to be more random than that.

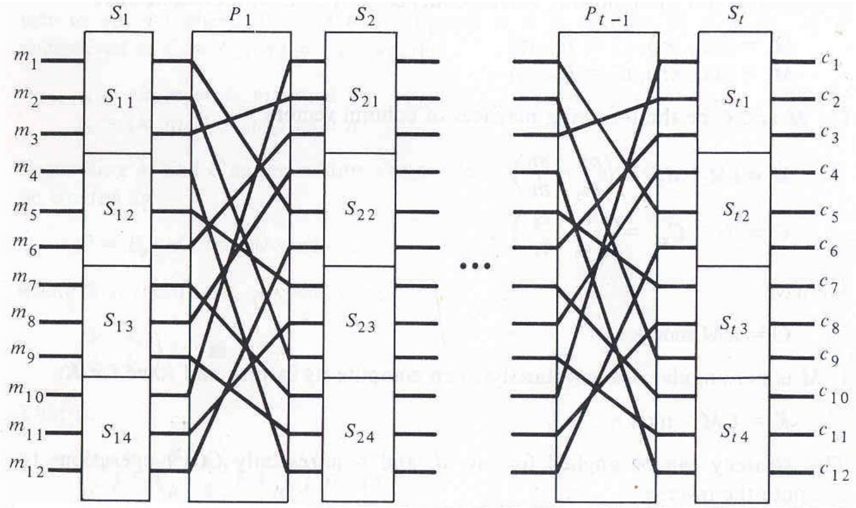
One-Time Pads

- Adding a plaintext and a completely random (not pseudo-random!) string of text characters modulo m yields an unconditionally secure cryptosystem.
- Main problem: Needs the same amount of secret key as plaintext to be encrypted.
- Never use the same pad twice, otherwise this system is easily broken.

Product Cipher

- Encrypt by alternately applying substitutions and transpositions (or permutations) to blocks of characters or bits over several rounds.
- Examples: DES (data encryption standard, 1977), and AES (advanced encryption standard, 2001).

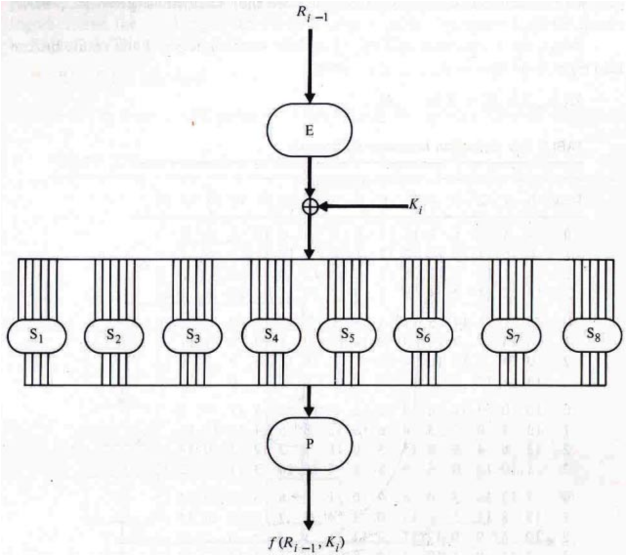
Substitution-Permutation Cipher



DES (Data Encryption Standard)

- Originally specified in FIPS 46 (Federal Information Processing Standard), 1977
- Reaffirmed in FIPS 46-3, 1999
- Encrypts and decrypts blocks of 64 bits under a 56-bit key
- Single DES encryption is no longer considered secure. Triple DES encryption is recommended.

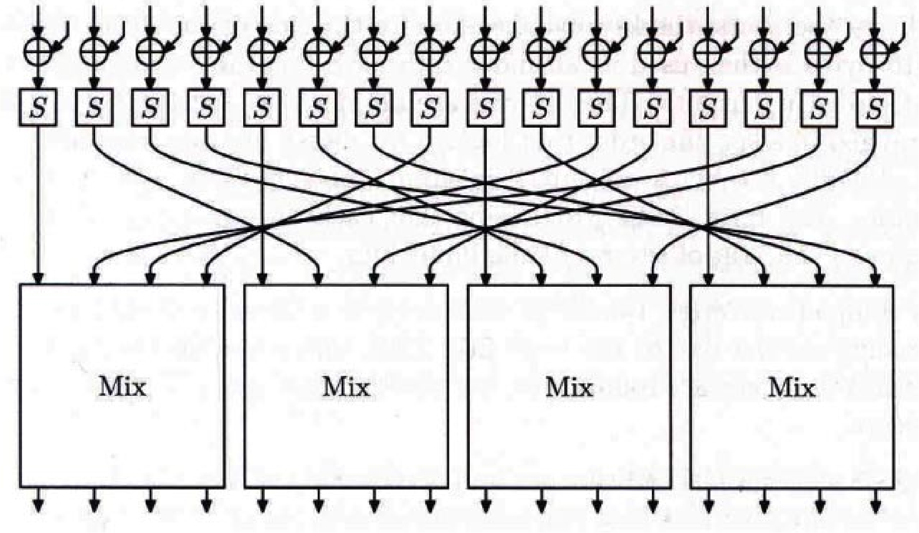
DES: 1 of 16 Rounds



AES (Advanced Encryption Standard)

- Specified in FIPS 197 (Federal Information Processing Standard), 2001
- Encrypts and decrypts 128 bit blocks under a key of size 128, 192, or 256 bits
- Depending on the key size 10, 12, or 14 rounds of encryption are used

AES: 1 of 10, 12, or 14 Rounds


S
Mix
Mix
Mix
Mix