بسم الله الرحمن الرحیم

مبانی رایانش امن

جلسه ۳

مجتبی خلیلی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان

مقدمه

- محرمانگی

مقدمه

- رمزنگاری (Cryptography):
  - داده‌های حساس را برای حمله کننده به صورت غیرقابل خواندن در میاورد.
  - از آن برای اطمینان از صحت داده استفاده می‌شود.
  - به کاربران غیرمجاز، اجازه دسترسی به سیستم را نمی دهد.

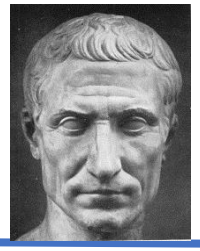
مقدمه

- در سرویس‌ها و مکانیزم‌های امنیتی، شاهد الگوریتم‌های مهم رمزنگاری خواهید بود. برخی از این الگوریتم‌ها که در این درس به صورت مقدماتی با آنها آشنا می‌شویم عبارتند از:
  - رمزگذاری متقارن
  - رمزگذاری کلید عمومی (نامتقارن)
  - امضای دیجیتال
  - تابع هش (درهم ساز- چکیده‌ساز)

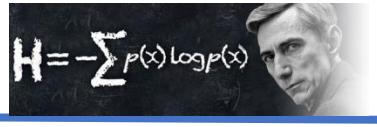
مقدمه

IUT-ECE

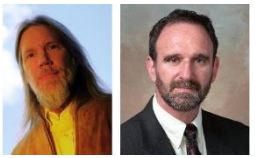
Caesar Cipher
(50 BC)



Shannon Entropy(~1950)



Cipher Machines (1900s)

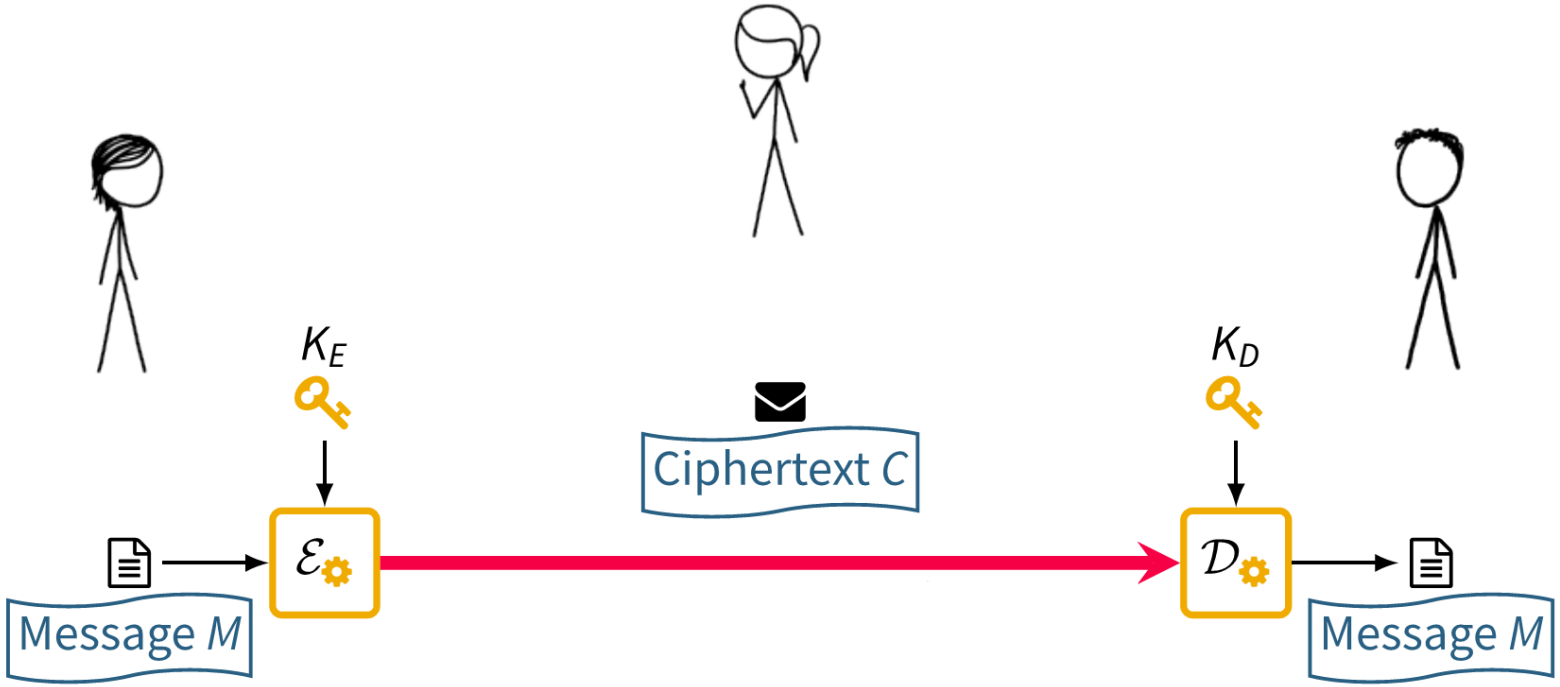


Public Key Crypto/RSA
1970s

تعاریف اولیه

- Plaintext: متن آشکار، همان پیام اصلی که هنوز رمز نشده است.
- Ciphertext: متن رمز شده،
- Key: یک مقدار مخفی که تنها فرستنده (و گاها گیرنده) میداند و از آن برای رمز کردن (و یا رمزگشایی) پیام استفاده می‌کند.
- Cipher یا Cryptosystem: الگوریتمی که کلید مخفی و پیام اصلی را می‌گیرد و متن رمز شده را برمیگرداند.

تعاریف اولیه



- فعلا محرمانگی. الزامات دیگر را در ادامه درس خواهیم دید.

مثال کلاسیک

مثال کلاسیک

- الگوریتم رمز سزار: این الگوریتم، یک الگوریتم شیفت است که هدف آن رمز کردن پیام‌های متنی است.
- کلید: (سه تا شیفت)

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

- مثال:

Plaintext: four score and seven years ago

Ciphertext: IRXUVFRUHDQGVHYHQBHDUVDJR

مثال کلاسیک

- اکنون قصد داریم ببینیم یک حمله کننده چگونه میتواند این الگوریتم رمز را بشکند و محرمانگی داده‌ها را نقض کند. هدف تعیین شانس پیروزی دشمن است. به این کار تحلیل رمز یا Cryptanalysis گویند.

مثال کلاسیک

- اولین راهی که به ذهن ما میرسد، جستجوی کامل فضای کلید است (Brute force).
- در حالت شیفت ساده، فضای کلید چقدر است؟(البته فرض اولیه معلوم بودن الگوریتم رمز برای حمله کننده است)

26

- فضای کلید چقدر باشد کافی است؟

مثال کلاسیک

- در حالت کلی به جای یک شیفت ساده، از یک جاینشینی استفاده می‌شود.
- برای مثال:

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

- مثال:

Plaintext: four score and seven years ago

Ciphertext: STPFC….

مثال کلاسیک

- در حالت جانشینی، فضای کلید چقدر است؟

$$26! > 2^{88}$$

- جستجوی کلید در این فضا نیاز به زمان بسیار زیادی دارد.

- اگر فضای کلید به اندازه کافی بزرگ باشد آنگاه میتوان نتیجه گرفت که الگوریتم رمز امن است؟

- الگوریتم رمز امن، الگوریتمی است که تنها حمله شناخته شده به آن، جستجوی کامل باشد.

مثال کلاسیک

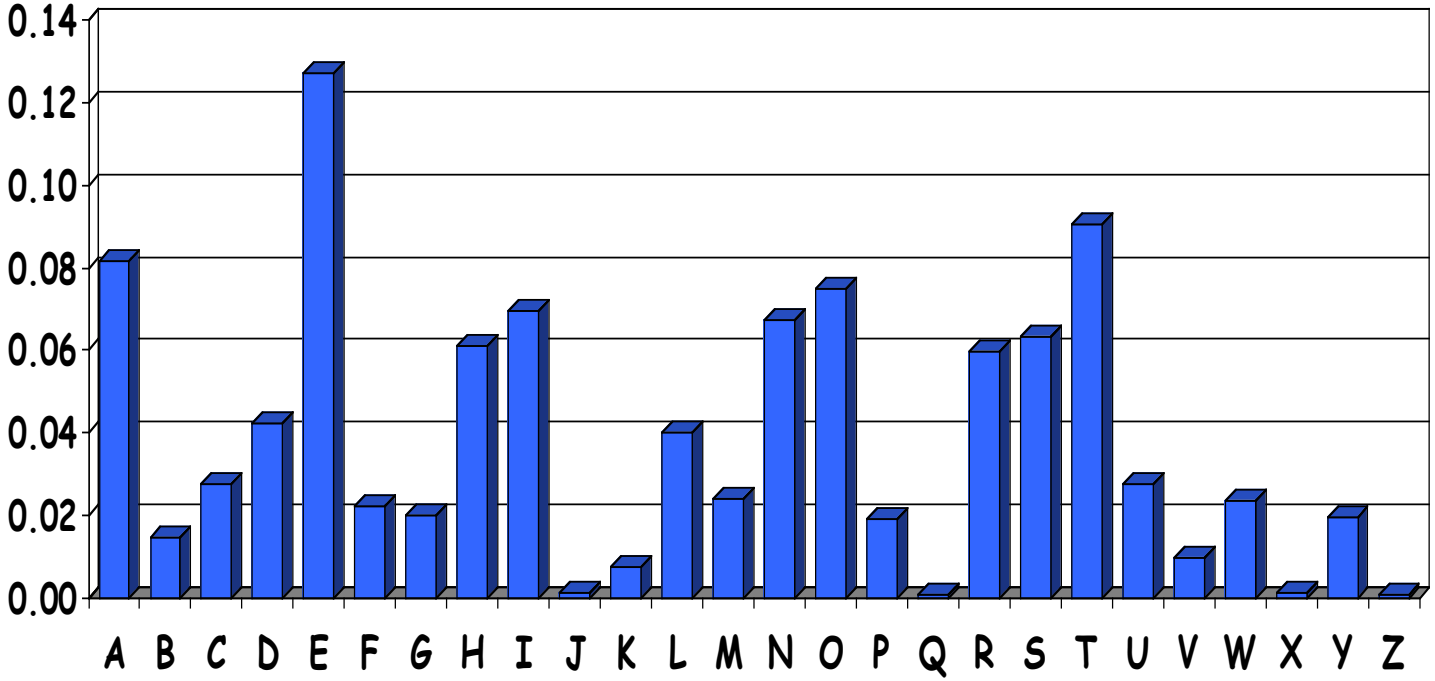
- آیا راه بهتری برای تحلیل الگوریتم رمز جانشینی هست؟
- با داشتن متن رمز شده زیر کلید را بیابید:

TNYH YH K HGXAGT RGHHKLG GVXECGC SHYVL K HYRZIG HSMHTYTSTYEV XYZNGA

مثال کلاسیک

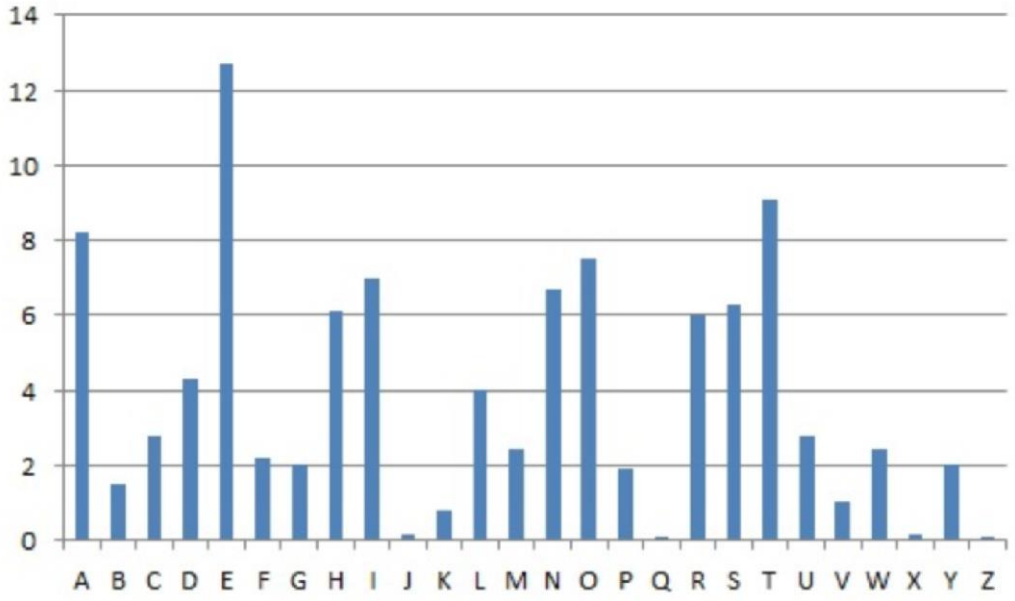
IUT-ECE

- تحلیل فرکانس تکرار حروف یا ترکیبات آنها

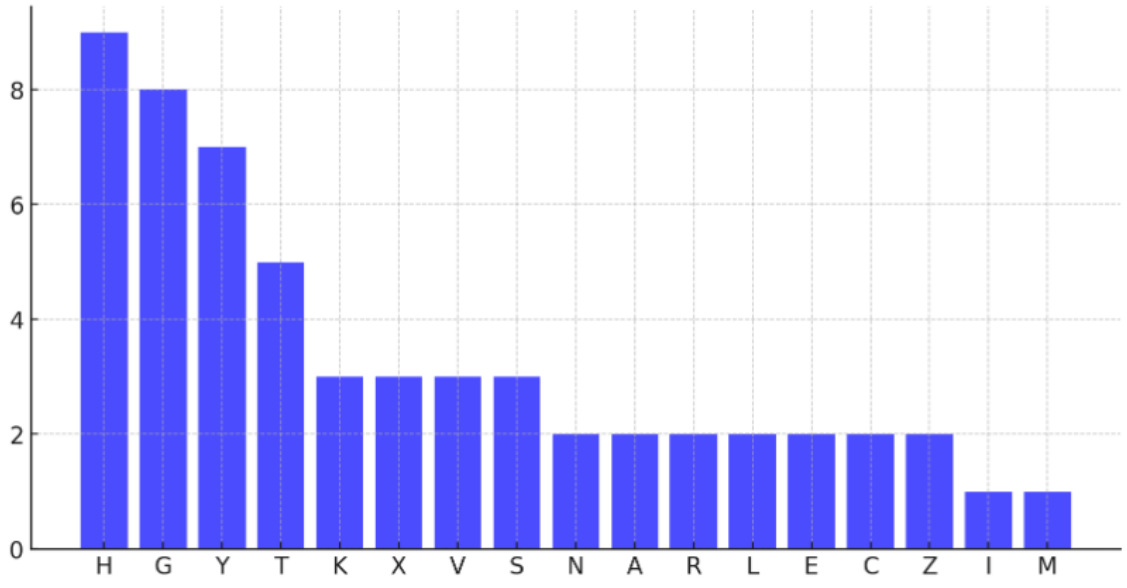


ابویوسف کندی-قرن سوم هجری ---- متاثر از خلیل بن احمد فراهیدی

مثال کلاسیک



فرکانس حروف انگلیسی (استاندارد)



فرکانس حروف انگلیسی در متن رمز شده مورد نظر

مثال کلاسیک

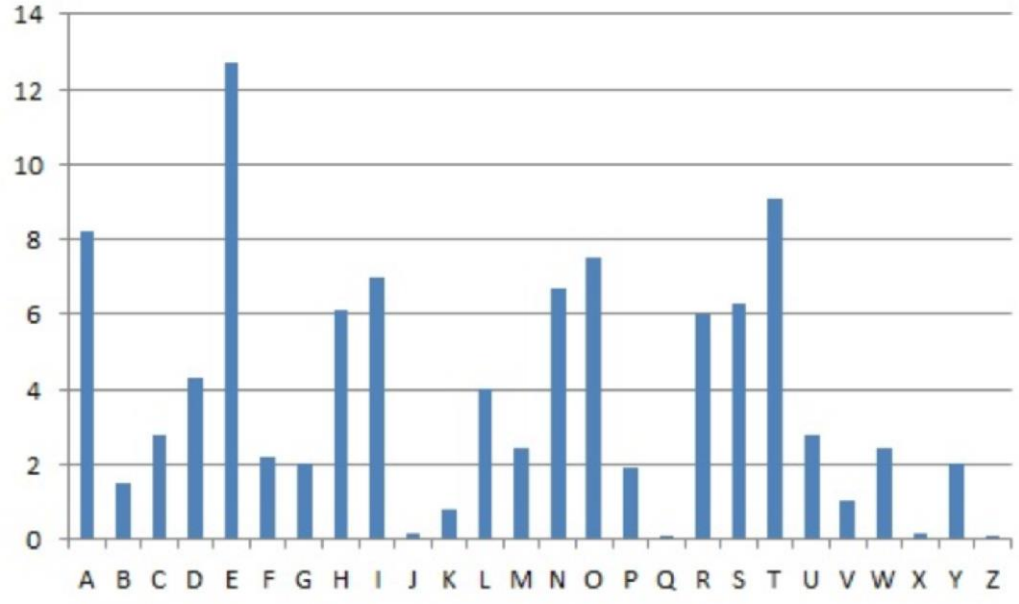
IUT-ECE

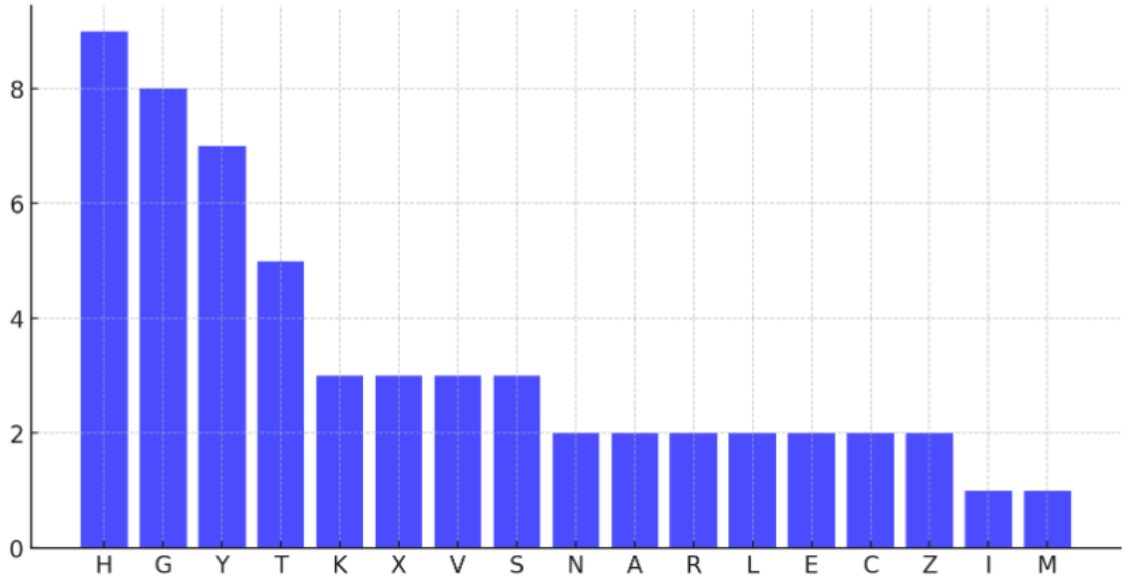
- تحلیل فرکانس تکرار حروف یا ترکیبات آنها

TNYH YH K HGXAGT RGHHKLG GVXECGC SHYVL K HYRZIG HSMHTYTSTYEV XYZNGA

بدست آوردن فرکانس حروف در متن رمز شده بالا و مقایسه با نمودار صفحه قبل

مثال کلاسیک





H → E

G → A

Y → I

T → T

مثال کلاسیک

IUT-ECE

TNYH YH K HGXAGT RGHHKLG GVXECGC SHYVL K HYRZIG HSMHTYTSTYEV XYZNGA

TNIE IE H EAOKAT RAEEHLA ASOECAC SEISL H EIRZIA ESMETITSTIES OIZNAK

THIS IS A SECRET MESSAGE ENCODED USING A SIMPLE SUBSTITUTION CIPHER

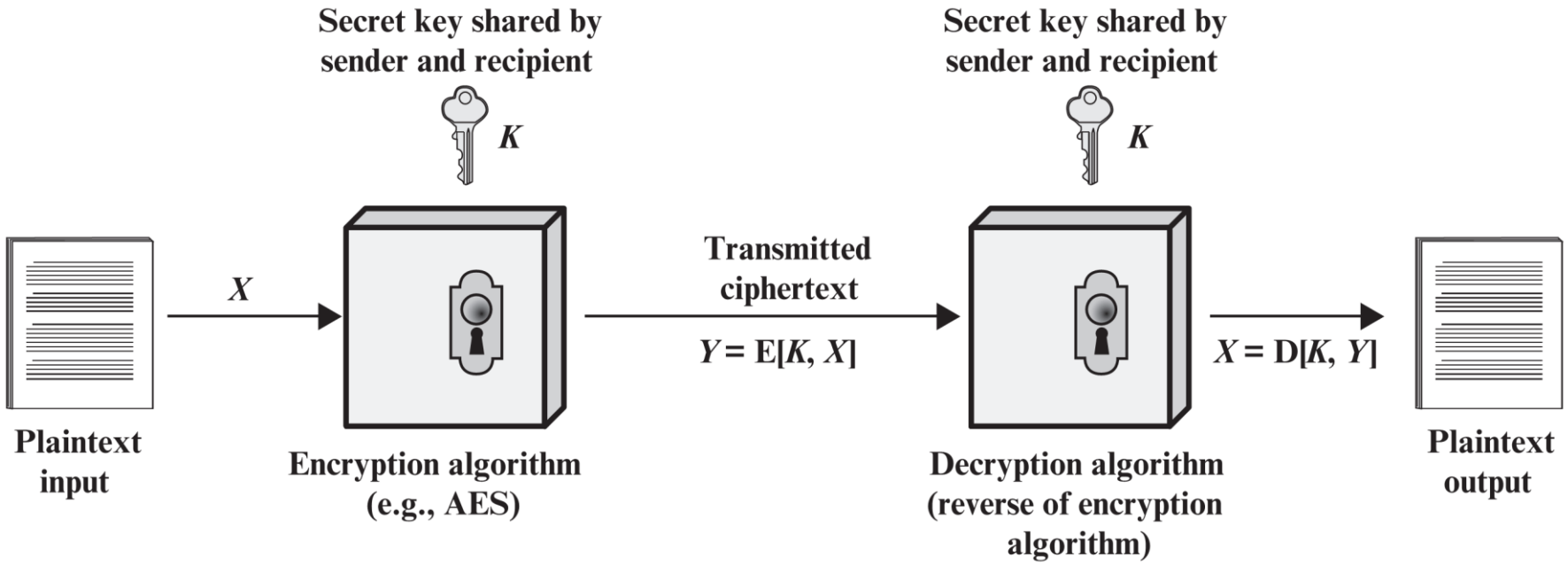
اصل Kerckhoffs (1883)

- این اصل بیان میکند که یک الگوریتم رمز باید امن باقی بماند حتی اگر دشمن هر اطلاعی بجز دانش کلید خصوصی را داشته باشد. یعنی:

  - دشمن الگوریتم رمز را میداند و ما با این فرض سیستم رمزگذار را طراحی میکنیم. تنها کلید مخفی است.

رمزنگاری متقارن

- گیرنده و فرستنده یک کلید مخفی مشترک دارند (اشتراک کلید از طریق کانال امن).



رمزنگاری متقارن

- در ادامه برخی از مهترین الگوریتم‌های رمز متقارن را بررسی میکنیم.
  - رمز یکبار مصرف (one-time-pad)
  - DES
  - AES
  - رمزهای جریانی

One-Time Pad (OTP)

- در جنگ جهانی دوم، کلود شانون بر روی یک سیستم رمز صوت کار میکرد. این امر موجب شد او پایه گذار تئوری اطلاعات و فرمول بندی ریاضیات ارتباطات شود.

ماکزیمم امنیت زمانی حاصل میشود که کلید کاملا رندوم باشد، یکبار استفاده شود و طول آن برابر طول متن اصلی باشد.

One-Time Pad

One-Time Pad (OTP)

- OPT تضمین ۱۰۰ درصدی امنیت میدهد به شرط آنکه تولید کلید به صورت کاملا رندوم باشد و تنها یک بار استفاده شود.

Encryption: Plaintext ⊕ Key = Ciphertext

Plaintext:	001	000	010	100	001	010	111	100	000	101
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	110	101	100	001	110	110	111	001	110	101

One-Time Pad (OTP)

Decryption: Ciphertext ⊕ Key = Plaintext

Ciphertext:	110	101	100	001	110	110	111	001	110	101
Key:	111	101	110	101	111	100	000	101	110	000
Plaintext:	001	000	010	100	001	010	111	100	000	101

One-Time Pad (OTP)

- در حالی که OTP تنها الگوریتمی است که تضمین امنیت کامل میدهد دارای عیوبی نیز هست:
  - نیاز به همگام سازی دارد.
  - طول کلید بسیار بزرگ
  - کلید نمیتواند باز استفاده شود.
  - مدیریت کلید سخت