مبانی رایانش امن
رمزنگاری- روش‌های متقارن

محسن هوشمند
دانشکده تکنولوژی اطلاعات و علم رایانه
دانشگاه تحصیلات تکمیلی علوم پایه زنجان

مقدمه- رمزنگاری

تبدیل داده به متن رمزی صرفا قابل خواندن برای فرستنده و گیرنده
- کلید key یا cipher هر روش تبدیل

امن کردن ذخیره اطلاعات و ارسال اطلاعات

عرضهٔ چهار بعد کلیدی از شش بعد امنیت
- یکپارچگی پیام
  - عدم تغییر پیام
- عدم‌انکار
  - عدم‌انکار ارسال پیام
- احراز هویت
  - تشخیص هویت فرد یا رایانه
- محرمانگی
  - اطمینان از نخواندن غیر

دارای سابقه
- جانشینی substitution
- جابجایی transposition

مقدمه- رمزنگاری متقارن

رمزنگاری متقارن

رمزنگاری معمول

رمزنگاری تک کلید

معمول‌ترین رمزنگاری‌ها تا قبل از کلید عمومی

بیشترین استفاده در مقایسه با دیگر نوع‌ها حتی کلید عمومی

مطالب مربوط به رمزنگاری متقارن

معرفی مدل عمومی فرایند رمزنگاری متقارن

رمزنگاری‌های متقارن پیش از رایانه

استگانوگرافی

استانداۀ رمزنگاری داده (ارد) DES

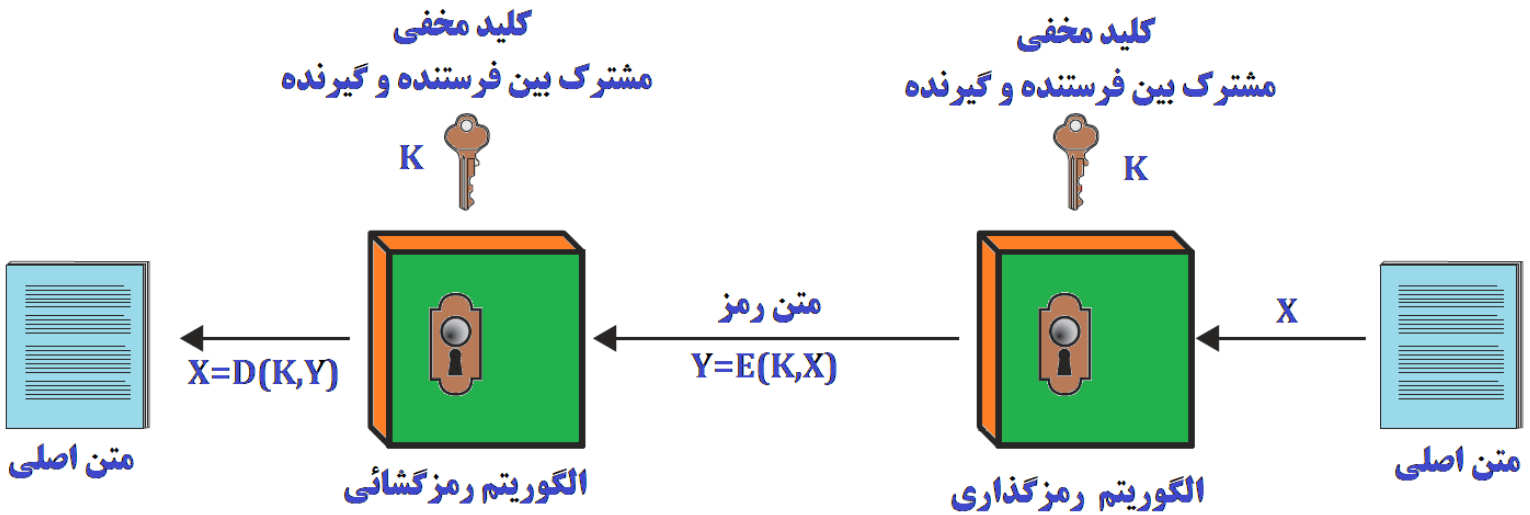
استانداۀ رمزنگاری پیشرفته (ارپ) AES

مقدمه-چند اصطلاح

- متن اصلی
  - Plaintext
  - پیام اصلی که قرار بر رمز شدن آن است
- متن رمز
  - Ciphertext
  - پیام در قالب رمز شده
  - در قالب لاطائلات!
- رمزگذاری (رمز)
  - Enciphering یا Encryption
  - فرایند تبدیل متن اصلی به متن رمز
- رمزگشائی (کشف)
  - Deciphering یا Decryption
  - فرایند بازسازی متن اصلی از متن رمز

- رمزنگاری
  - Cryptography
  - Cipher یا Cryptographic system
  - روش‌ها و طرح‌های مختلف مورد استفاده در ناخوانا کردن پیام و بازسازی پیام اصلی
- تحلیل رمز
  - Cryptoanalysis
  - رمزشکنی یا کشف رمز
  - رمزگشائی پیام بدون دانشی درباره نحوهٔ رمزگذاری
- رمزشناسی
  - Cryptology
  - رمزنگاری و تحلیل‌رمز توأمان

رمزگذاری متقارن- بنیادها



متن اصلی

الگوریتم رمزگذاری
- با جانشینی و جابجائی

کلید رمز
- ورودی الگوریتم رمزنگاری
- تغییر کلید موجب تغییر در خروجی
- اکثر یا همهٔ عملیات‌ها وابسته به کلید

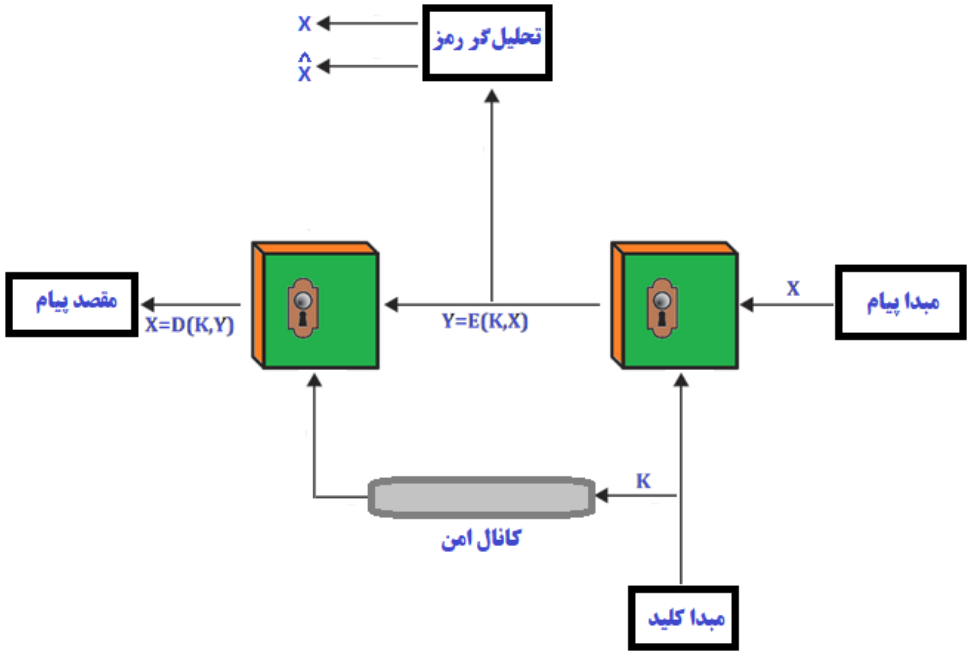
متن رمز
- حاصل دو کلید متفاوت ⟸ دو متن رمز متفاوت
- دنباله‌ای تصادفی از داده‌ها

الگوریتم رمزگشائی
- معمولا الگوریتم رمزگذاری با ترتیب معکوس در اجرا
- ورودی متن رمز و کلید رمز

رمزنگاری متقارن- نیازمندی‌ها

الگوریتم رمزگذاری قوی

داشتن نسخهٔ یکسان از کلید رمز با روشی امن



امنیت رمزگذاری وابسته به کلید تا الگوریتم

به دیگر سخن، عدم نیاز به مخفی داشتن الگوریتم و کافی بودن مخفی داشتن کلید

معیارهای طبقه‌بندی روش‌های رمزگذار

الف- نوع عملیات تبدیل

- مبنی بر دو اصل عمومی
  - جانشینی substitution
  - نگاشت هر نویسهٔ متن اصلی به عنصری دیگر
  - جابجائی transposition
  - تغییر ترتیب نویسه‌های متن اصلی
  - سیستم‌های ترکیبی
  - چند مرحله از جانشینی و جابجائی

ب- تعداد کلید مورداستفاده

- استفادهٔ فرستنده و گیرنده از کلید یکسان ⟸ رمزنگاری متقارن، تک-کلید، کلید-مخفی، معمول
- استفادهٔ فرستنده و گیرنده از کلیدهای متفاوت⟸ رمزنگاری نامتقارن، دو-کلید، کلید-عمومی

ج- روش پردازش متن

- رمز بلوکی
  - پردازش یک بلوک و دسته از داده‌ها در هر زمان
- رمز دنباله‌ای
  - پردازش پیوستهٔ داده‌های ورودی
  - تولید یک خروجی در هر زمان

انواع حمله به متن رمز شده

تحلیل رمز

تکیه بر

نوع الگوریتم

اطلاعی عمومی از نویسه‌های متن اصلی

چند جفت متن اصلی-متن رمز متناظر

استفاده از اطلاعات مذکور جهت استنتاج متن اصلی یا کلید رمز

حمله جستجو کامل

امتحان همهٔ کلیدهای ممکن بر متن رمز تا یافتن متن اصلی

میانگین تلاش- نیمی از کلیدها

تحلیل رمز

فرض بر دانستن الگوریتم‌های رمزگذاری و رمزگشائی

- در پی یافتن متن اصلی
- یا متن اصلی و کلید هر دو

انواع تحلیل رمز

مبنی بر میزان اطلاع

- سخت‌ترین- صرفا وجود متن رمز
- گاهی اوقات دانستن الگوریتم رمزنگاری
  - امتحان تمامی کلیدها
  - بزرگی فضای کلید، غیرعملی شدن
- اعمال روش‌های آماری
  - نیاز به دانستن کلیتی از متن اصلی
  - (انگلیسی، فارسی، فایل اجرائی، متن جاوا، فایل حسابداری، امثالهم)
- اطلاع از تکرار الگو در متن اصلی
  - پست‌اسکریپت دارای الگوئی تکراری در شروع فایل
  - سرهای استانده
  - متن اصلی معلوم
- حملهٔ کلمه-محتمل
  - دانستن بخشی از محتوای پیام
  - حملهٔ متن‌اصلی انتخابی
  - «تحلیل رمز تفاضلی»

نوع حمله	اطلاعات در دسترس تحلیل‌گر رمز
صرفا متن‌رمز	• الگوریتم رمزگذاری • متن رمز
متن اصلی دانسته	• الگوریتم رمزگذاری • متن رمز • چند جفت متن‌اصلی-متن رمز
متن اصلی انتخابی	• الگوریتم رمزگذاری • متن رمز • متن اصلی انتخابی تحلیل‌گر به همراه متن رمز متناظر آن
متن‌رمز انتخابی	• الگوریتم رمزگذاری • متن رمز • متن رمز انتخابی تحلیل‌گر به همراه متن اصلی متناظر آن
متن انتخابی	• الگوریتم رمزگذاری • متن رمز • متن اصلی انتخابی تحلیل‌گر به همراه متن رمز متناظر آن • متن رمز انتخابی تحلیل‌گر به همراه متن اصلی متناظر آن

انواع تحلیل رمز

بی‌قید-امن unconditionally secure

- نبود اطلاع کافی در متن رمز برای یافتن الگو در متن اصلی
- استقلال از میزان امکانات و زمان در اختیار
- نبود چنین الگوریتمی در عمل
  - چرخاندن روی از جای «امنیت بی‌قید و شرط» به «رایانشی-امن»

رایانشی-امن ← در صورت برآورده شدن یکی از دو شرط زیر

- بیشتر بودن هزینهٔ شکستن رمز از ارزش اطلاع رمز شده
- بیشتر بودن زمان موردنیاز جهت شکستن رمز از عمر مفید استفاده از اطلاع

حمله جستجو کامل

میانگین امتحان کلیدها برابر نصف تعداد کلیدها

نیاز به روشی جهت تشخیص متن اصلی

- فارسی، انگلیسی
- خودکارسازی

تشخیص سخت‌تر با فشرده‌سازی پیام پیش از رمزنگاری

- سخت‌تر شدن خودکارسازی

مکمل روش جستجو کامل

- درجه‌ای از اطلاع از متن اصلی

روش رمزهای سنتی- معرفی چند نمونه

ویژگی‌ها

- از زمرهٔ روش‌های کلید متقارن
- صرفا وجه محرمانگی داده
- روش‌های متقدم مبنی بر الفبا
  - روش‌های جدید مبنی بر اطلاع دودوئی
  - مبتنی بر جانشینی و جابجائی
- فن‌های جانشینی
  - جانشینی حروف متن با حروف دیگر یا اعداد یا نمادها
  - در صورت دودوئی بودن
  - جانشینی الگوهای دودویی متن اصلی با الگوهای دودوئی

ا ب پ ت ث ج چ ح خ د ذ ر ز ژ س ش ص ض ط ظ ع غ ف ق ک گ ل م ن و ه ی

ت ث ج چ ح خ د ذ ر ز ژ س ش ص ض ط ظ ع غ ف ق ک گ ل م ن و ه ی ا ب پ

روش‌های جانشینی

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

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

meet me after the session

PHHW PH DIWHU WKH VHVVLRQ

روش سزار

- به نظر قدیمی‌ترین و ساده‌ترین
  - روش رمز جابجائی
  - از نوع جانشینی هر حرف با حرفی دیگر
  - بین صفر تا ۳۱ در رسم‌الخط فارسی و صفر تا ۲۵ در رسم‌الخط انگلیسی
  - جانشینی حرف با حرفی با سه فاصله از آن
  - غیرامن

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
۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴	۲۵

تعمیم روش سزار

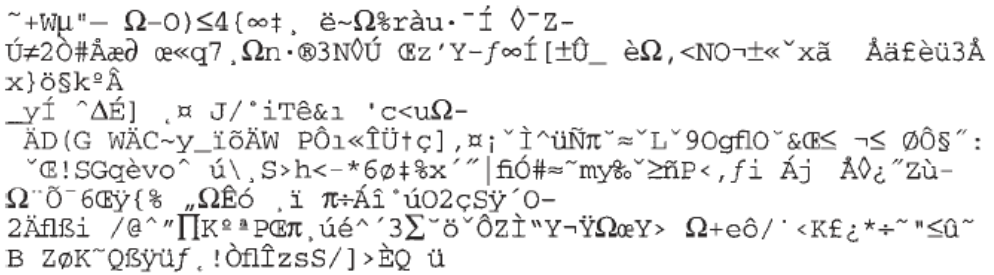
- در صورت دانستن روش سزار
- الگوریتم امتحان تمام کلیدها در فارسی یا انگلیسی

رمزگذاری	الفبای لاتین جابجائی سه حرفی	$C = E(۳, p) = (p + ۳)\%۲۶$
	الفبای لاتین جابجائی به اندازه کلید k	$C = E(k, p) = (p + k)\%۲۶$
	الفبای فارسی جابجائی سه حرفی	$C = E(۳, p) = (p + ۳)\%۳۲$
	الفبای فارسی جابجائی به اندازه کلید k	$C = E(k, p) = (p + k)\%۳۲$
رمزگشائی	الفبای لاتین جابجائی به اندازه کلید k	$p = D(k, p) = (C - k)\%۲۶$
	الفبای فارسی جابجائی به اندازه کلید k	$p = D(k, p) = (C - k)\%۳۲$

روش‌های جانشینی

دلایل امکان تحلیلی رمز جستجو کامل

- شناخته بودن الگوریتم‌های رمزگذاری و رمزگشائی
  - چنین بودن در تقریبا تمامی اوقات
- نیاز به امتحان صرفا ۳۲ یا ۲۶ کلید
  - از دلایل غیرممکنی جستجوی کامل- تعداد زیاد کلید
- مشخص بودن زبان متن اصلی
  - کمک ناشناخته بودن متن اصلی به تشخیص‌ناپذیری متن اصلی خروجی
  - فشرده‌سازی



ا ب پ ت ث ج چ ح خ د ذ ر ز ژ س ش ص ض ط ظ ع غ ف ق ک گ ل م ن و ه ی

چ ط ع ق م غ و ب ر گ ث ه ن ف ا خ ح ت ک ض ج پ ی ظ ر ش ز ذ س ژ ل ص

روش رمزهای سنتی- تک الفبائی

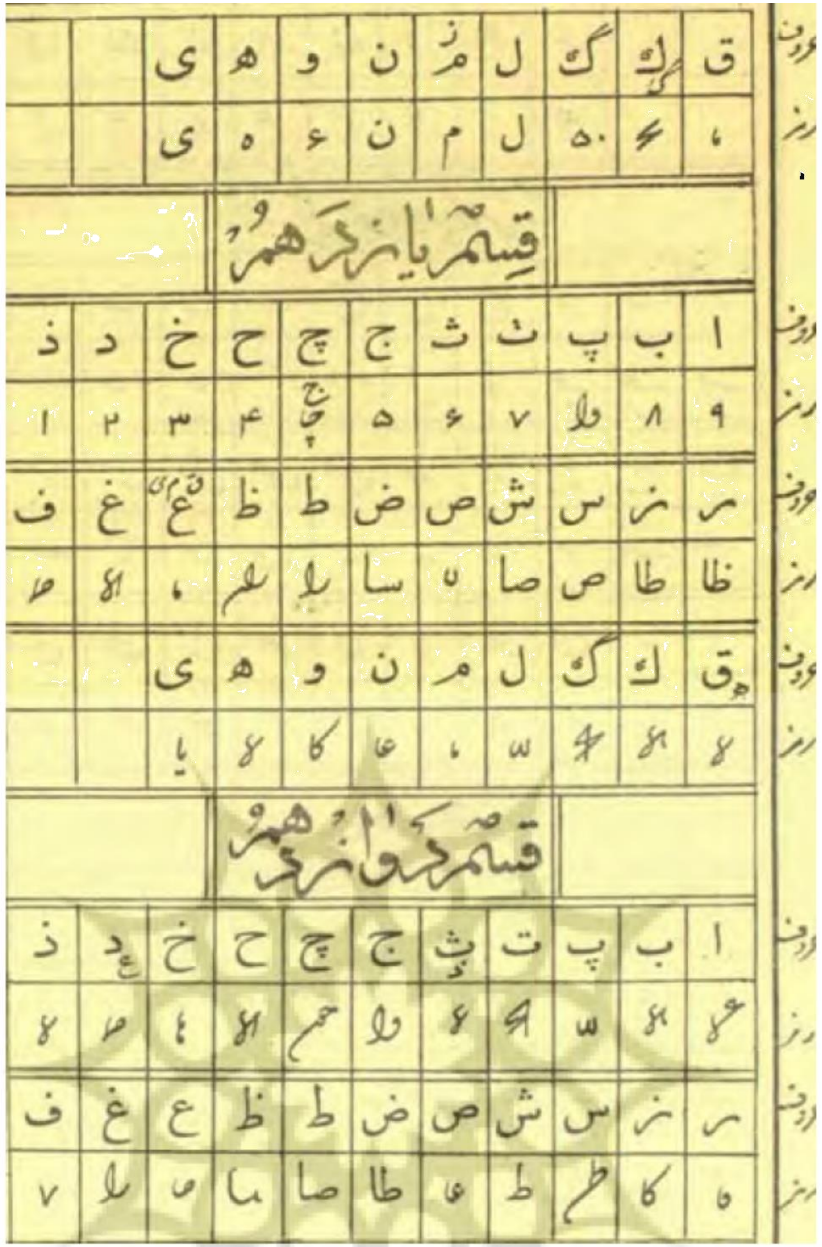
- روش جانشینی ساده
  - استفاده از جایگشتی دلبخواه از نویسه‌های الفبا
  - جهت ۳۲ حرف دارای !۳۲ جایگشت ممکن
    - جایگشت؟
  - امکان افزودن کلیدهای بیشتر با افزودن اعداد و دیگر علائم
  - حتی بزرگتر از فضای جستجوی ارد
- روش جانشینی تک-حرفی (تک الفبائی)
- اما در صورت انتخاب جایگشت‌های واضح، بالا بودن احتمال شکست
  - با دانستن الگوهای زبان اصلی

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

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

روش رمزهای سنتی- تک

- روش قائم مقام
- روش یوسفی
- رمز ناصری



نمونه‌ای از اقلام اختراعی قائم مقام فراهانی همراه با کلید رمز(مفتاح‌الملک: ۱۳۲۰: ۲۹)

روش رمزهای سنتی- تک الفبائی

A	۸/۱۶۷	N	۶/۷۴۹
B	۱/۴۹۲	O	۷/۵۰۷
C	۲/۷۸۲	P	۱/۹۲۹
D	۴/۲۵۳	Q	۰/۰۹۵
E	۱۲/۷۰۲	R	۵/۹۸۷
F	۲/۲۲۸	S	۶/۳۲۷
G	۲/۰۱۵	T	۹/۰۵۶
H	۶/۰۹۴	U	۲/۷۵۸
I	۶/۹۹۶	V	۰/۹۷۸
J	۰/۱۵۳	W	۲/۳۶۰
K	۰/۷۷۲	X	۰/۱۵۰
L	۴/۰۲۵	Y	۱/۹۷۴
M	۲/۴۰۶	Z	۰/۰۷۴

- رمز جانشینی تک‌الفبائی
  - monoalphabetic substitution cipher
- امکان حمله؟
  - نوعی دیگری از حملات
  - در صورت اطلاع تحلیل‌گر رمز از نوع متن اصلی
  - استخراج الگوها از زبان
    - مقایسه با بسامد تکرار حروف در زبان اصلی
    - مناسب در صورت طولانی بودن متن رمز
  - قدم بعد
  - اختصاصی دلخواه
  - روشمندتر: بدنبال الگوهای دیگر، کلمات بسامد بالا در زبان، م.ث.، روش دی‌گرم (DIGRAM)

روش رمزهای سنتی- تک الفبائی

A	۸/۱۶۷	N	۶/۷۴۹
B	۱/۴۹۲	O	۷/۵۰۷
C	۲/۷۸۲	P	۱/۹۲۹
D	۴/۲۵۳	Q	۰/۰۹۵
E	۱۲/۷۰۲	R	۵/۹۸۷
F	۲/۲۲۸	S	۶/۳۲۷
G	۲/۰۱۵	T	۹/۰۵۶
H	۶/۰۹۴	U	۲/۷۵۸
I	۶/۹۹۶	V	۰/۹۷۸
J	۰/۱۵۳	W	۲/۳۶۰
K	۰/۷۷۲	X	۰/۱۵۰
L	۴/۰۲۵	Y	۱/۹۷۴
M	۲/۴۰۶	Z	۰/۰۷۴

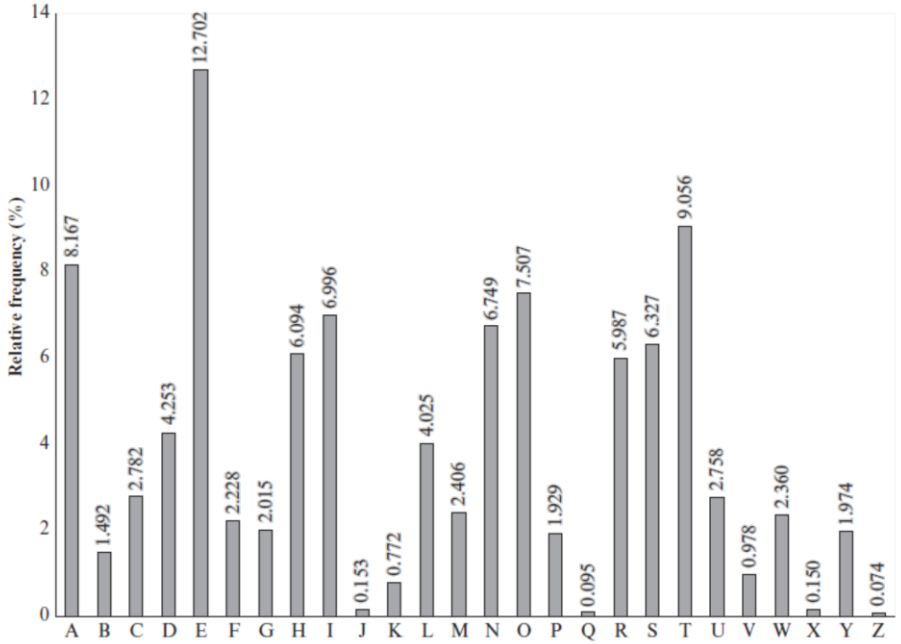


Figure 3.5 Relative Frequency of Letters in English Text

- رمز جانشینی تک‌الفبائی
  - monoalphabetic substitution cipher
- امکان حمله؟
  - نوعی دیگری از حملات
  - در صورت اطلاع تحلیل‌گر رمز از نوع متن اصلی
  - استخراج الگوها از زبان
    - مقایسه با بسامد تکرار حروف در زبان اصلی
    - مناسب در صورت طولانی بودن متن رمز
  - قدم بعد
    - اختصاصی دلخواه
    - روشمندتر: بدنبال الگوهای دیگر، کلمات بسامد بالا در زبان، م.ث.، روش دی‌گرم (DIGRAM)

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

روش رمزهای سنتی- تک الفبائی- جانشینی

P	۱۳/۳۳	H	۵/۸۳	F	۳/۳۳	B	۱/۶۷	C	0
Z	۱۱/۶۷	D	۵/۰۰	W	۳/۳۳	G	۱/۶۷	K	0
S	۸/۳۳	E	۵/۰۰	Q	۲/۵۰	Y	۱/۶۷	L	0
U	۸/۳۳	V	۴/۱۷	T	۲/۵۰	I	۰/۸۳	N	0
O	۷/۵۰	X	۴/۱۷	A	۱/۶۷	J	۰/۸۳	R	0
M	۶/۶۷								

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
t e e te a that e e a a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
e t ta t ha e ee a e th t a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
e e e tat e the t

it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow

روش رمزهای سنتی

- رمز تک‌الفبائی
  - ساده جهت شکستن
  - انعکاس بسامد الفباء اصلی
- راه حل-
  - روش‌های هم‌واجی (هوموفون‌ها)
    - اختصاص چند کد رمز به تک نویسه
    - تخصیص هر کد تصادفا یا دورا
    - باور گاوس شهیر به شکست‌ناپذیری رمز مذکور
    - اما صرفا تاثیر بر تک علامت‌ها و نه الگوهای چند حرفی
  - رمزکردن چند حرف از متن اصلی
  - استفاده از چند رمز

روش رمزهای سنتی-پلی‌فر

https://en.wikipedia.org/wiki/Playfair_cipher

- رمز چندنویسه
- رمز پلی‌فر معروف‌ترین
  - در نظر گرفتن جفتی‌ها (دی‌گرم‌ها) به مثابهٔ تک واحد
  - رمز تک‌واحدها به جفتی‌های متن رمز
  - مخترع آن ویتستون اما مشهور به نام توزیع کنندهٔ آن پلی‌فر
- از نوع رمزگذاری جانشینی
  - استفاده از ماتریس ۵ × ۵ حروف
  - رمزکردن جفت حروف

روش رمزهای سنتی-پلی‌فر

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

الف- تولید ماتریس کلید ۵ × ۵

- هر درایه یک حرف
- هر خانه حرف منحصر به فرد
  - حروف I و J در یک خانه
- حروف ابتدایی در ماتریس حروف کلید، سپس بقیه حروف الفبا به ترتیب

روش رمزهای سنتی-پلی‌فر

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

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

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

ب- رمزگذاری

- تقسیم کلمه به قطعات دو حرفی
  - در صورت فرد بودن افزودن z به قطعه آخر
  - Mohsen به mo و hs و en
- جفت‌ها نباید یکی باشند
  - Hello به he و lx و lo
- قواعد رمزگذاری
  - هر دو حرف در یک ستون
    - جاگذاری حرف زیر هر یک
    - ME به CL
  - هر دو حرف در یک ردیف
    - جاگذاری حرف سمت راست هر یک
    - ST به TL
  - در غیر صورت‌های بالا
    - تشکیل مستطیل و برداشتن از گوشه‌های مخالف افقی
    - NT به RQ

روش رمزهای سنتی-پلی‌فر

- هر دو حرف در یک ستون
  - جاگذاری حرف بالای هر یک
  - CL به ME
- هر دو حرف در یک ردیف
  - جاگذاری حرف سمت چپ هر یک
  - TL به ST
- در غیر صورت‌های بالا
  - تشکیل مستطیل و برداشتن از گوشه‌های مخالف افقی
  - RQ به NT

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

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

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

روش رمزهای سنتی-پلی‌فر

- استانداردِ ارتش بریتانیا در جنگ جهانی اول
- استفادهٔ امریکا و متفقین از آن در طول جنگ دوم جهانی
- جهت محافظت از داده‌های مهم ولی غیرامن

- مزایا
  - کلیدهای بیشتر ۶۲۵ مورد جفت-نویسا به جای ۲۵ مورد تک‌نویسا
  - معرفی به عنوان غیرقابل شکست
  - نیاز به متن رمز بیشتر جهت شکستن رمز در روش تحلیل بسامدی
- معایب
  - خود معکوسی جانشینی

روش رمزهای سنتی

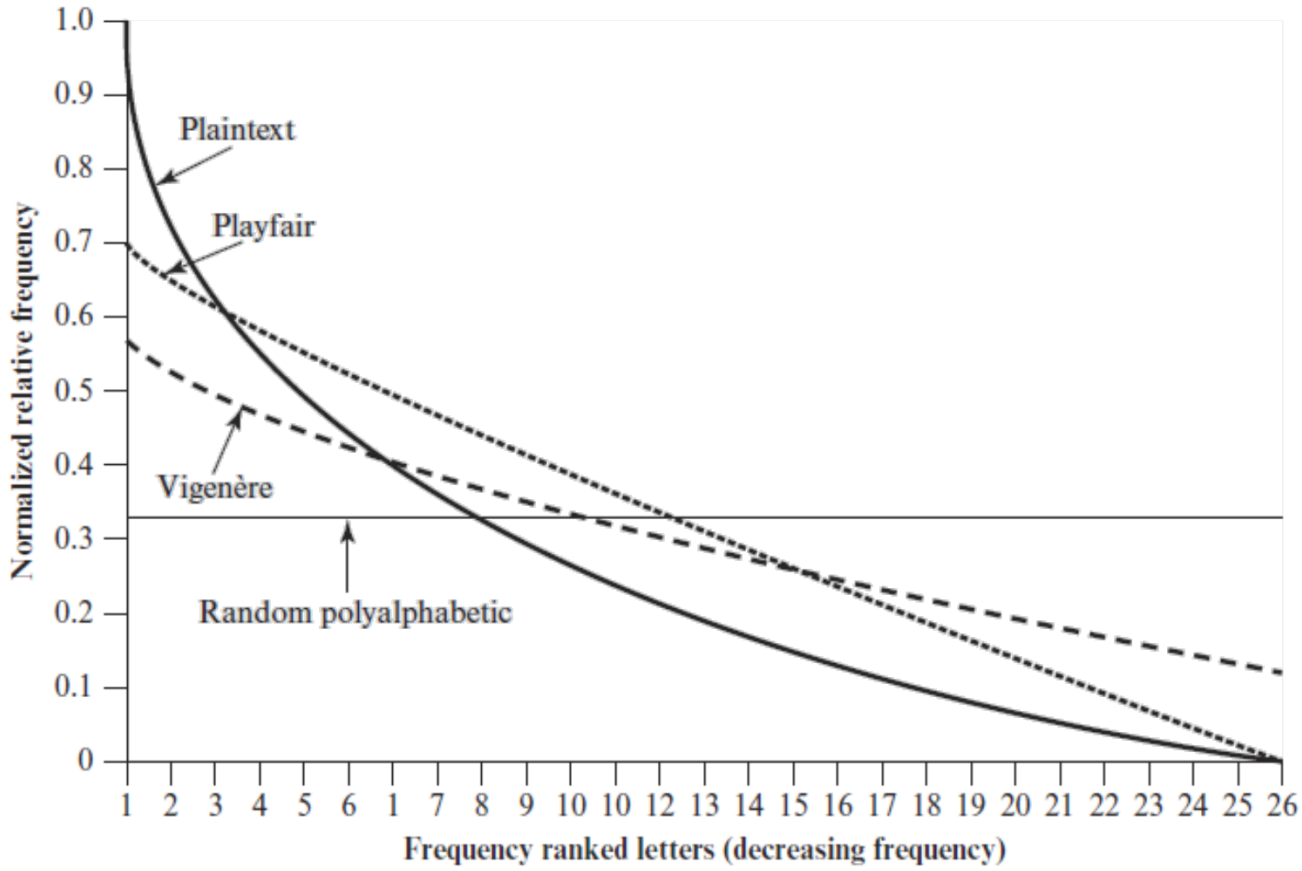


Figure 3.6 Relative Frequency of Occurrence of Letters

یادآوری و چند نکتهٔ جدید

ریاضی (حساب) پیمانه‌ای

پیمانه

mod

عدد صحیح a و عدد طبیعی n، آنگاه $a \,\%\, n$ برابر است با باقیمانده تقسیم a بر n

یادآوری الگوریتم تقسیم:

$$a = qn + r, \qquad 0 \le r < n; q = \left\lfloor \frac{a}{n} \right\rfloor$$

تغییر نمایش

$$a = \left\lfloor \frac{a}{n} \right\rfloor \times n + a \,\%\, n$$

نمایش صوری عملگر پیمانه

$$a \,\%n = a \; - \left\lfloor \frac{a}{n} \right\rfloor \times n, n \neq 0$$

$$۱۱ \,\%۷ = ۴,$$
$$-۱۱\%۷ = ۳\; n$$

رابطه هم‌نهشتی پیمانه

اظهار اینکه دو ورودی دارای باقیماندهٔ یکسان با توجه به پیمانه داده شده

- مثال (۳ پیمانه)۴ ≡ ۷ یا $۷ \equiv ۴ (mod ۳)$ یا ۴ $\overset{۳}{\equiv}$ ۷
  - هر دوی ۷ و ۴ دارای باقیماندهٔ ۱ به هنگام تقسیم بر ۳
- هم‌ارزی دو رابطهٔ زیر:

$$۷ \equiv ۴ \left(\text{۳ پیمانه}\right) \Leftrightarrow ۷\%\ ۳ = ۴\%\ ۳$$

- به سخن دیگر، یکسانی $a \equiv b (m$ پیمانه$)$ با مضرب صحیح بودن $a - b$ از m

≡ علامت هم‌نهشتی

استفاده از رابطه هم‌نهشتی در تعریف رده‌های افراز باقی‌مانده‌ها

- اعدادی با باقیمانده یکسان به پیمانه m تشکیل‌دهندهٔ یک رده به پیمانهٔ m
- وجود m رده (کلاس) به پیمانهٔ m

عمل‌های حساب پیمانه‌ای

مجموعه اعداد طبیعی کوچکتر از n

$$Z_n = \{0,1, \dots, n-1\}$$

- مشهور به مجموعه باقی‌مانده‌ها به پیمانهٔ n
  - هر عدد نمایش یک رده
  - نمایش با $[0]$ و $[1]$ و $[2]$ و ... و $[n-1]$ به طوری که

$$[r] = \{a : a \in Z, a\}$$

- رده‌های مانده به پیمانهٔ ۴

$$[0] = \{\dots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \dots\}$$
$$[1] = \{\dots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \dots\}$$
$$[2] = \{\dots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \dots\}$$
$$[3] = \{\dots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \dots\}$$

- انتخاب کوچکترین عدد نامنفی به عنوان نشان رده

رابطه هم‌نهشتی پیمانه

ویژگی‌ها

$$I.\quad m|(a-b) \Longrightarrow a \overset{m}{\equiv} b$$

$$II.\quad a \overset{m}{\equiv} a$$

$$III.\quad a \overset{m}{\equiv} b \Longrightarrow b \overset{m}{\equiv} a$$

$$IV.\quad a \overset{m}{\equiv} b, b \overset{m}{\equiv} c \Longrightarrow a \overset{m}{\equiv} c$$

$$V.\quad a \overset{m}{\equiv} b, c \overset{m}{\equiv} d \Longrightarrow \begin{cases} a+c \overset{m}{\equiv} b+d \\ ac \overset{m}{\equiv} bd \end{cases}$$

$$VI.\quad a \overset{m}{\equiv} b \Longrightarrow a^k \overset{m}{\equiv} b^k$$

موارد II و III و IV به ترتیب نمایش خاصیت‌های بازتابی و تقارن و تراگذری- بنابراین هم‌نهشتی رابطه‌ای هم‌ارزی است.

عمل‌های حساب پیمانه‌ای

عملگر پیمانه m

- نگاشت کنندهٔ تمامی اعداد صحیح به مجموعه‌های $\{0,1, \dots ,(m-1)\}$
- پرسش: امکان تعریف عملیات‌های ریاضی که محدود به مجموعه باقی بمانند.
  - پاسخ مثبت و در روشی به نامه حساب پیمانه‌ای
  - دارای ویژگی‌های

$$[a \,\%\, m + b \,\%\, m]\%\, m = (a+b)\%\, m$$
$$[a \,\%\, m - b \,\%\, m]\%\, m = (a-b)\%\, m$$
$$[a \,\%\, m \times b \,\%\, m]\%\, m = (a \times b)\%\, m$$

  - مورد اول $a \,\%\, m = r_a$ و $b \,\%\, m = r_b$
  - $\Longleftarrow$ $a = r_a + jm$ و $b = r_b + km$

$$(a+b)\%\, m = (r_a + jm + r_b + km)\%\, m$$
$$= (r_a + r_b)\%\, m$$
$$= [a \,\%\, m + b \text{ پیمانه } m]\%\, m$$

عمل‌های ریاضیات پیمانه‌ای

مثال- $۳ = ۸ \% ۱۱$ و $۷ = ۸ \% ۱۵$

$$[(۱۱ \% ۸) + (۱۵ \% ۸)] \% ۸ = ۱۰ \% ۸ = ۲$$
$$(۱۱ + ۱۵) \% ۸ = \% ۸ = ۲$$

$$[(۱۱ \% ۸) - (۱۵ \% ۸)] \% ۸ = -۴ \% ۸ = ۴$$
$$(۱۱ - ۱۵) \% ۸ = -۴ \% ۸ = ۴$$

$$[(۱۱ \% ۸) \times (۱۵ \% ۸)] \% ۸ = ۲۱ \% ۸ = ۵$$
$$(۱۱ \times ۱۵) \% ۸ = ۱۶۵ \% ۸ = ۵$$

عمل‌های ریاضیات پیمانه‌ای

مثال-توان‌رسانی

- $۱۱^{۷} \% ۱۳ = ۲$
- با ضرب متوالی

$$۱۱^{۲} = ۱۲۱ \overset{۱۳}{\equiv} ۴$$

$$۱۱^{۴} = \left(۱۱^{۲}\right)^{۲} \overset{۱۳}{\equiv} ۴^{۲} \overset{۱۳}{\equiv} ۳$$

$$۱۱^{۷} = ۱۱ \times ۱۱^{۲} \times ۱۱^{۴}$$

$$۱۱^{۷} \overset{۱۳}{\equiv} ۱۱ \times ۴ \times ۳ \overset{۱۳}{\equiv} ۲$$

عمل‌های ریاضیات پیمانه‌ای

مثال-

عملیات‌ها به پیمانهٔ ۸

+	۰	۱	۲	۳	۴	۵	۶	۷
۰	۰	۱	۲	۳	۴	۵	۶	۷
۱	۱	۲	۳	۴	۵	۶	۷	۰
۲	۲	۳	۴	۵	۶	۷	۰	۱
۳	۳	۴	۵	۶	۷	۰	۱	۲
۴	۴	۵	۶	۷	۰	۱	۲	۳
۵	۵	۶	۷	۰	۱	۲	۳	۴
۶	۶	۷	۰	۱	۲	۳	۴	۵
۷	۷	۰	۱	۲	۳	۴	۵	۶

جمع به پیمانهٔ ۸

×	۰	۱	۲	۳	۴	۵	۶	۷
۰	۰	۰	۰	۰	۰	۰	۰	۰
۱	۰	۱	۲	۳	۴	۵	۶	۷
۲	۰	۲	۴	۶	۰	۲	۴	۶
۳	۰	۳	۶	۱	۴	۷	۲	۵
۴	۰	۴	۰	۴	۰	۴	۰	۴
۵	۰	۵	۲	۷	۴	۱	۶	۳
۶	۰	۶	۴	۲	۰	۶	۴	۲
۷	۰	7	۶	۵	۴	۳	۲	۱

ضرب به پیمانهٔ ۸

توجه به تفاوت رفتاری جمع و ضرب

w	$-w$	w^{-1}
۰	۰	–
۱	۷	۱
۲	۶	–
۳	۵	۳
۴	۴	–
۵	۳	۵
۶	۲	–
۷	۱	۷

معکوس جمع و ضرب به پیمانهٔ ۸

عمل‌های ریاضیات پیمانه‌ای

مثال-

عملیات‌ها به پیمانهٔ ۷

+	0	1	2	3	4	5	6
0	0	۱	۲	۳	۴	۵	۶
۱	۱	۲	۳	۴	۵	۶	0
۲	۲	۳	۴	۵	۶	0	۱
۳	۳	۴	۵	۶	0	۱	۲
۴	۴	۵	۶	0	۱	۲	۳
۵	۵	۶	0	۱	۲	۳	۴
۶	۶	0	۱	۲	۳	۴	۵

جمع به پیمانهٔ ۷

×	0	۱	۲	۳	۴	۵	۶
0	0	0	0	0	0	0	0
۱	0	۱	۲	۳	۴	۵	۶
۲	0	۲	۴	۶	۱	۳	۵
۳	0	۳	۶	۲	۵	۱	۴
۴	0	۴	۱	۵	۲	۶	۳
۵	0	۵	۳	۱	۶	۴	۲
۶	0	۶	۵	۴	۳	۲	۱

ضرب به پیمانهٔ ۷

w	$-w$	$w^{-۱}$
0	0	–
۱	۶	۱
۲	۵	۴
۳	۴	۵
۴	۳	۲
۵	۲	۳
۶	۱	۱

معکوس جمع و ضرب به پیمانهٔ ۷

عمل‌های حساب پیمانه‌ای

- ویژگی‌های حساب پیمانه‌ای اعداد طبیعی در Z_n
  - قوانین جابجاپذیری

$$(w + x)\%n = (x + w)\%n$$
$$(w \times x)\%n = (x \times w)\%n$$

  - قوانین شرکت‌پذیری

$$[(w + x) + y]\%n = [w + (x + y)]\%n$$
$$[(w \times x) \times y]\%n = [w \times (x \times y)]\%n$$

  - قوانین توزیع‌پذیری

$$[w \times (x + y)]\%n = [w \times x + w \times y]\%n$$

  - عضوهای همانی

$$(0 + x)\%n = (x)\%n$$
$$(۱ \times x)\%n = (x)\%n$$

  - معکوس جمع $(-w)$

$$\forall w \in Z_n : \exists z \Longrightarrow w + z \overset{n}{\equiv} 0$$

عمل‌های حساب پیمانه‌ای

ویژگی حساب پیمانه‌ای متفاوت از ریاضی معمول

- همانند جمع معمولی

$$(a+b) \overset{n}{\equiv} (a+c) \Rightarrow b \overset{n}{\equiv} c$$
$$(۵+۲۳) \overset{n}{\equiv} (۵+۷) \Rightarrow ۲۳ \overset{n}{\equiv} ۷$$

- اما ضرب متفاوت! درستی رابطه زیر در صورتی که دو عدد صحیح نسبت به هم اول باشند.

$$\left[\text{ب‌م‌م}(a,n) = ۱, (a \times b) \overset{n}{\equiv} (a \times c)\right] \Rightarrow b \overset{n}{\equiv} c$$

- مثالی جهت درست نبودن ضرب در هر حالتی

$$۶ \times ۳ = ۱۸ \overset{۸}{\equiv} ۲$$
$$۶ \times ۷ = ۴۲ \overset{۸}{\equiv} ۲$$

اما $۳ \overset{۸}{\not\equiv} ۷$

عمل‌های حساب پیمانه‌ای

- اما ضرب متفاوت! درستی رابطه زیر در صورتی که دو عدد صحیح نسبت به هم اول باشند.

$$\left[\text{ب‌م‌م}(a,n) = ۱, (a \times b) \overset{n}{\equiv} (a \times c)\right] \Longrightarrow b \overset{n}{\equiv} c$$

دلیل

- هر پیمانهٔ n و ضریب a جهت تولید اعداد 0 تا $n - ۱$
  - شکست در تولید مجموعهٔ تمام مانده‌ها اگر a و n دارای شمارندهٔ مشترک باشند.

عمل‌های حساب پیمانه‌ای

- $a = ۶$ و $n = ۸$

$Z_۸$	۷	۶	۵	۴	۳	۲	۱	0
ضرب در ۶	۴۲	۳۶	۳۰	۲۴	۱۸	۱۲	۶	0
مانده‌ها	۲	۴	۶	0	۲	۴	۶	0

- $a = ۵$ و $n = ۸$

$Z_۸$	۷	۶	۵	۴	۳	۲	۱	0
ضرب در ۶	۳۵	۳۰	۲۵	۲۰	۱۵	۱۰	۵	0
مانده‌ها	۳	۶	۱	۴	۷	۲	۵	0

- عدد صحیحی دارای «معکوس ضربی» در Z_n است اگر و فقط اگر عدد مذکور نسبت به n اول باشد.

معکوس ماتریس مربع

معکوس ماتریس A^{-1}

$$AA^{-1} = A^{-1}A = I$$

رمزگذاری چندالفبائی- رمز هیل

$$A = \begin{bmatrix} ۵ & ۸ \\ ۱۷ & ۳ \end{bmatrix}$$

- دترمینان

$$\begin{vmatrix} ۵ & ۸ \\ ۱۷ & ۳ \end{vmatrix} = ۵ \times ۳ - ۸ \times ۱۷ = -۱۲۱ \% ۲۶ = ۹$$

- معادلهٔ محاسبهٔ معکوس عبارت است از

$$A^{-۱} = \frac{۱}{۹} \begin{bmatrix} ۳ & -۸ \\ -۱۷ & ۵ \end{bmatrix}$$

- اما در اینجا نیاز به استفاده از خاصیت پیمانه‌ای

$$۹^{-۱} \% ۲۶ = ۳ \Leftrightarrow ۹ \times ۳ = ۲۷ \% ۲۶ = ۱$$

- آشنایی با عنوان- «الگوریتم اقلیدس افزوده» روشی برای محاسبهٔ معکوس پیمانه‌ای
  - تدریس در صورت لزوم

$$A = \begin{bmatrix} ۵ & ۸ \\ ۱۷ & ۳ \end{bmatrix} \Rightarrow A^{-۱} \% ۲۶ = ۳ \begin{bmatrix} ۳ & -۸ \\ -۱۷ & ۵ \end{bmatrix} = \begin{bmatrix} ۹ & ۵۴ \\ ۲۷ & ۱۵ \end{bmatrix} = \begin{bmatrix} ۹ & ۲ \\ ۱ & ۱۵ \end{bmatrix}$$

رمزگذاری چندالفبائی- رمز هیل

- یاداوری در صورت معکوس پذیر بودن ماتریس

$$A = \begin{bmatrix} ۵ & ۸ \\ ۱۷ & ۳ \end{bmatrix}$$

$$A^{-۱} \text{٪} ۲۶ = \begin{bmatrix} ۹ & ۲ \\ ۱ & ۱۵ \end{bmatrix}$$

$$AA^{-۱} \text{٪} ۲۶ = \begin{bmatrix} ۵ \times ۹ + ۸ \times ۱ & ۵ \times ۲ + ۸ \times ۱۵ \\ ۱۷ \times ۹ + ۳ \times ۱ & ۱۷ \times ۲ + ۳ \times ۱۵ \end{bmatrix} = \begin{bmatrix} ۵۳ & ۱۳۰ \\ ۱۵۶ & ۷۹ \end{bmatrix} \%۲۶ = \begin{bmatrix} ۱ & 0 \\ 0 & ۱ \end{bmatrix}$$

- دترمینان- برابر جمع تمامی حاصلضرب‌هایی تشکیل شده از استفاده از دقیقا یک عضو از هر ردیف و یک عضو از هر ستون
  - در هر حالی بعضی از ضرب‌ها منفی شوند.

رمزگذاری چندالفبائی- رمز هیل

$$A = \begin{bmatrix} ۵ & ۸ \\ ۱۷ & ۳ \end{bmatrix}$$

$$\begin{vmatrix} ۵ & ۸ \\ ۱۷ & ۳ \end{vmatrix} = ۵ \times ۳ - ۸ \times ۱۷ = -۱۲۱ \% ۲۶ = ۹$$

- معادلهٔ محاسبهٔ معکوس عبارت است از

$$A^{-۱} = \frac{۱}{۹} \begin{bmatrix} ۳ & -۸ \\ -۱۷ & ۵ \end{bmatrix}$$

- اما در اینجا نیاز ه استفاده از خا یت پیمانه‌ای

$$۹^{-۱} \% ۲۶ = ۳ \Leftrightarrow ۹ \times ۳ = ۲۷ \% ۲۶ = ۱$$

- آشنایی با عنوان- الگوریتم اقلیدس افزوده روشی برای محاسبهٔ معکوس پیمانه‌ای
  - تدریس در صورت لزوم

$$A = \begin{bmatrix} ۵ & ۸ \\ ۱۷ & ۳ \end{bmatrix} \Rightarrow A^{-۱} \% ۲۶ = ۳ \begin{bmatrix} ۳ & -۸ \\ -۱۷ & ۵ \end{bmatrix} = \begin{bmatrix} ۹ & ۵۴ \\ ۲۷ & ۱۵ \end{bmatrix} = \begin{bmatrix} ۹ & ۲ \\ ۱ & ۱۵ \end{bmatrix}$$

رمزگذاری چندالفبائی- رمز هیل

رمز چندحرفی

ریاضیدانی به نام لستر هیل
- ۱۹۲۹

رمزگذاری
- دریافت m حرف پشت سرهم متن اصلی و جانشینی آن‌ها با m متن رمز
- با m معادلهٔ خطی
- مثال- $m = ۳$

$$c_۱ = (k_{۱۱}p_۱ + k_{۲۱}p_۲ + k_{۳۱}p_۳)\%۲۶$$
$$c_۲ = (k_{۱۲}p_۱ + k_{۲۲}p_۲ + k_{۳۲}p_۳)\%۲۶$$
$$c_۳ = (k_{۱۳}p_۱ + k_{۲۳}p_۲ + k_{۳۳}p_۳)\%۲۶$$

- نمایش ماتریسی

$$(c_۱, c_۲, c_۳) = (p_۱, p_۲, p_۳)\begin{pmatrix} k_{۱۱} & k_{۱۲} & k_{۱۳} \\ k_{۲۱} & k_{۲۲} & k_{۲۳} \\ k_{۳۱} & k_{۳۲} & k_{۳۳} \end{pmatrix}\%۲۶$$
$$\boldsymbol{c} = \boldsymbol{p}K\%۲۶$$

رمزگذاری چندالفبائی- رمز هیل

رمزگذاری

- دریافت m حرف پشت سرهم متن اصلی و جانشینی آن‌ها با m متن رمز
- با m معادلهٔ خطی
- مثال- $m = ۳$

$$c_۱ = (k_{۱۱}p_۱ + k_{۲۱}p_۲ + k_{۳۱}p_۳)\%۲۶$$
$$c_۲ = (k_{۱۲}p_۱ + k_{۲۲}p_۲ + k_{۳۲}p_۳)\%۲۶$$
$$c_۳ = (k_{۱۳}p_۱ + k_{۲۳}p_۲ + k_{۳۳}p_۳)\%۲۶$$

رمزگذاری چندالفبائی- رمز هیل

رمزگذاری

- دریافت m حرف پشت سرهم متن اصلی و جانشینی آن‌ها با m متن رمز
- با m معادلهٔ خطی
- مثال- $m = ۳$

$$c_۱ = (k_{۱۱}p_۱ + k_{۲۱}p_۲ + k_{۳۱}p_۳)\%۲۶$$
$$c_۲ = (k_{۱۲}p_۱ + k_{۲۲}p_۲ + k_{۳۲}p_۳)\%۲۶$$
$$c_۳ = (k_{۱۳}p_۱ + k_{۲۳}p_۲ + k_{۳۳}p_۳)\%۲۶$$

- نمایش ماتریسی

$$(c_۱, c_۲, c_۳) = (p_۱, p_۲, p_۳)\begin{bmatrix} k_{۱۱} & k_{۱۲} & k_{۱۳} \\ k_{۲۱} & k_{۲۲} & k_{۲۳} \\ k_{۳۱} & k_{۳۲} & k_{۳۳} \end{bmatrix}\%۲۶$$

$$\boldsymbol{c} = \boldsymbol{p}K\%۲۶$$

رمزگذاری چندالفبائی- رمز هیل

$$\mathrm{K} = \begin{bmatrix} ۱۷ & ۱۷ & ۵ \\ ۲۱ & ۱۸ & ۲۱ \\ ۲ & ۲ & ۱۹ \end{bmatrix}$$

$$\boldsymbol{p} = (۱۵, 0, ۲۴)$$

$$(۱۵, 0, ۲۴)K = (۳۳۱, ۳۰۳, ۵۳۱)\%۲۶ = (۱۷, ۱۷, ۱۱) = RRL$$

رمزگشائی استفاده از معکوس K

دترمینان برابر ۲۳ و

$$\mathrm{K}^{-۱} = \begin{bmatrix} ۴ & ۹ & ۱۵ \\ ۱۵ & ۱۷ & ۶ \\ ۲۴ & 0 & ۱۷ \end{bmatrix}$$

$$\mathrm{K} = \begin{bmatrix} ۱۷ & ۱۷ & ۵ \\ ۲۱ & ۱۸ & ۲۱ \\ ۲ & ۲ & ۱۹ \end{bmatrix} \begin{bmatrix} ۴ & ۹ & ۱۵ \\ ۱۵ & ۱۷ & ۶ \\ ۲۴ & 0 & ۱۷ \end{bmatrix} = \begin{bmatrix} ۴۴۳ & ۴۴۲ & ۴۴۲ \\ ۸۵۸ & ۴۹۵ & ۷۸۰ \\ ۴۹۴ & ۵۲ & ۳۶۵ \end{bmatrix} \%۲۶ = \begin{bmatrix} ۱ & 0 & 0 \\ 0 & ۱ & 0 \\ 0 & 0 & ۱ \end{bmatrix}$$

رمزگذاری چندالفبائی- رمز هیل

$$\mathbf{c} = \mathrm{E}(\mathrm{K}, \mathbf{p}) = \boldsymbol{p}K \% ۲۶$$
$$\mathbf{p} = \mathrm{D}(\mathrm{K}, \mathbf{c}) = \boldsymbol{c}K^{-۱} \% ۲۶ = \boldsymbol{p}KK^{-۱} = \boldsymbol{p}$$

رمزگذاری چندالفبائی- رمز هیل

پنهان کردن بسامدهای تک‌حرفی

ماتریس بزرگتر، مخفی شدن بیشتر بسامدها

- ماتریس سه در سه مخفی کنندهٔ بسامدهای یک و دو حرفی
  - استفاده از ماتریس بزرگتری مخفی کنندهٔ اطلاعات بسامدی بیشتر
- مقاوم در مقابل حمله صرفا متن رمز
- شکستن آسان در مقابل حمله «متن اصلی شناخته»

رمزگذاری چندالفبائی- رمز هیل

- رمز هیل $m \times m$
  - فرض بر وجود m جفت متن اصلی- متن رمز هر یک با طول m
    - $\boldsymbol{p_j} = (p_{1j}, p_{2j}, \dots, p_{mj})$
    - $\boldsymbol{c_j} = (c_{1j}, c_{2j}, \dots, c_{mj})$
    - ماتریس K مجهول

$$\Longrightarrow \forall 1 \leq j \leq m: \mathbf{c_j} = \boldsymbol{p_j} K$$

  - تعریف دو ماتریس $P = (p_{ij})$ و $C = (c_{ij})$، آن‌گاه داریم $C = PK$

$$\Longrightarrow K = P^{-1} C$$

  - در صورت معکوس‌ناپذیر بودن P، امکان یافتن نسخهٔ دیگری از ماتریس مذکور با افزودن جفت متن اصلی متن رمز تا معکوس‌پذیر شدن آن

رمزگذاری چندالفبائی- رمز هیل

- مثال
  - متن اصلی hillcipher و متن رمز HCRZSSXNSP
  - پس روشن شدن

$$(۷,۸)K\%۲۶ = (۷,۲)$$
$$(۱۱,۱۱)K\%۲۶ = (۱۷,۲۵)$$
$$\vdots$$

  - استفاده از دو جفت نخست متن-اصلی متن رمز، داریم:

$$\begin{bmatrix} ۷ & ۲ \\ ۱۷ & ۲۵ \end{bmatrix} = \begin{bmatrix} ۷ & ۸ \\ ۱۱ & ۱۱ \end{bmatrix} K\%۲۶$$

$$\begin{bmatrix} ۷ & ۲ \\ ۱۷ & ۲۵ \end{bmatrix}^{-۱} = \begin{bmatrix} ۲۵ & ۲۲ \\ ۱ & ۲۳ \end{bmatrix}$$

$$K = \begin{bmatrix} ۲۵ & ۲۲ \\ ۱ & ۲۳ \end{bmatrix} \begin{bmatrix} ۷ & ۲ \\ ۱۷ & ۲۵ \end{bmatrix} = \begin{bmatrix} ۵۴۹ & ۶۰۰ \\ ۳۹۸ & ۵۷۷ \end{bmatrix} \%۲۶ = \begin{bmatrix} ۳ & ۲ \\ ۸ & ۵ \end{bmatrix}$$

  - امکان آزمون درستی پاسخ با سایر جفت‌ها

روش رمزهای سنتی- رمزهای چندجانشینی

استفاده از چندجانشینی تک‌حرفی

کلیدی مشخص‌کننده قوانین انتخاب جانشینی

روش رمزهای سنتی-رمز ویژنه

- معروفترین و از موارد بسیار ساده
- نوعی دیگر از تعمیم روش سزار
- هر حرف کلیدی متفاوت

- شامل
  - متن اصلی
    - $\boldsymbol{p} = p_0 p_1 p_2 \dots p_{n-1}$
  - کلید
    - $\boldsymbol{k} = k_0 k_1 k_2 \dots k_{m-1}$ و $m < n$
  - متن رمز حاصل
    - $\boldsymbol{c} = c_0 c_1 c_2 \dots c_{n-1}$

Vigenère

https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

روش رمزهای سنتی-رمز ویژنه

- رمزگذاری

$$\boldsymbol{c} = [c_0, c_1, \dots, c_{n-1}] = E(\boldsymbol{k}, \boldsymbol{p}) = E\big[[k_0, k_1, \dots, k_{m-1}], [p_0, p_1, \dots, p_{n-1}]\big]$$
$$= (p_0 + k_0)\%26, (p_1 + k_1)\%26, \dots, (p_{m-1} + k_{m-1})\%26,$$
$$(p_m + k_0)\%26, (p_{m+1} + k_1)\%26, \dots, (p_{2m-1} + k_{m-1})\%26 \dots$$

$$c_i = (p_i + k_{i\%m})\%26$$

$$p_i = (c_i - k_{i\%m})\%26$$

Vigenère

https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

روش رمزهای سنتی-رمز ویژنه

- مثال- با کلید deceptive

کلید	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e
متن اصلی	w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s	a	v	e	y	o	u	r	s	e	l	f
متن رمز	Z	I	C	V	T	W	Q	N	G	R	Z	G	V	T	W	A	V	Z	H	C	Q	Y	G	L	M	G	J

- بیان عددی

کلید	۳	۴	۲	۴	۱۵	۱۹	۸	۲۱	۴	۳	۴	۲	۴	۱۵	۱۹	۸	۲۱	۴	۳	۴	۲	۴	۱۵	۱۹	۸	۲۱	۴
متن اصلی	۲۲	۴	0	۱۷	۴	۳	۸	۱۸	۲	۱۴	۲۱	۴	۱۷	۴	۳	۱۸	0	۲۱	۴	۲۴	۱۴	۲۰	۱۷	۱۸	۴	۱۱	۵
متن رمز	۲۵	۸	۲	۲۱	۱۹	۲۲	۱۶	۱۳	۶	۱۷	۲۵	۶	۲۱	۱۹	۲۲	0	۲۱	۲۵	۷	۲	۱۶	۲۴	۶	۱۱	۱۲	۶	۹

Vigenère

https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

روش رمزهای سنتی-رمز ویژنه

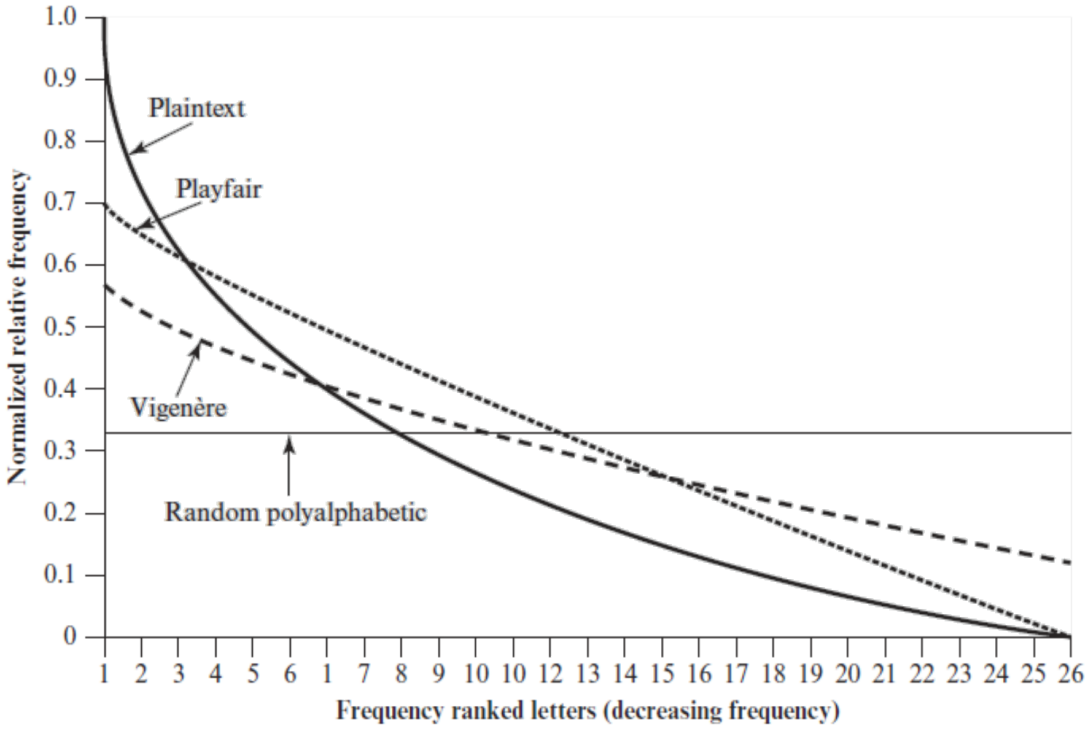


Figure 3.6 Relative Frequency of Occurrence of Letters

قدرت رمز

- وجود چند کلید، منحصر برای هر کلمه
  - مخفی کردن بسامد حرف

از بین نرفتن تمامی دانش ساختار متن اصلی

- شکل روبرو دانش ساختار باقی‌مانده پس از رمز با ویژنه با کلید به طول ۹
  - بهبود نسبت به پلی‌فیر
  - باقی‌ماندن دانش قابل‌توجهی از ساختار و بسامد

تلاشی بر شکستن رمز

- طول کلید
  - از بین بردن ذات متناوب کلید با استفاده از کلیدی بدون تکرار و دارای طولی برابر متن
  - سیستم خودکلید
- تمرین گروهی
  - مطالعه مقاله مم۹۳
  - بسامد حروف فارسی

Vigenère

Simmons, G. “Cryptology.” *Encyclopaedia Britannica*, *Fifteenth Edition*, 1993.

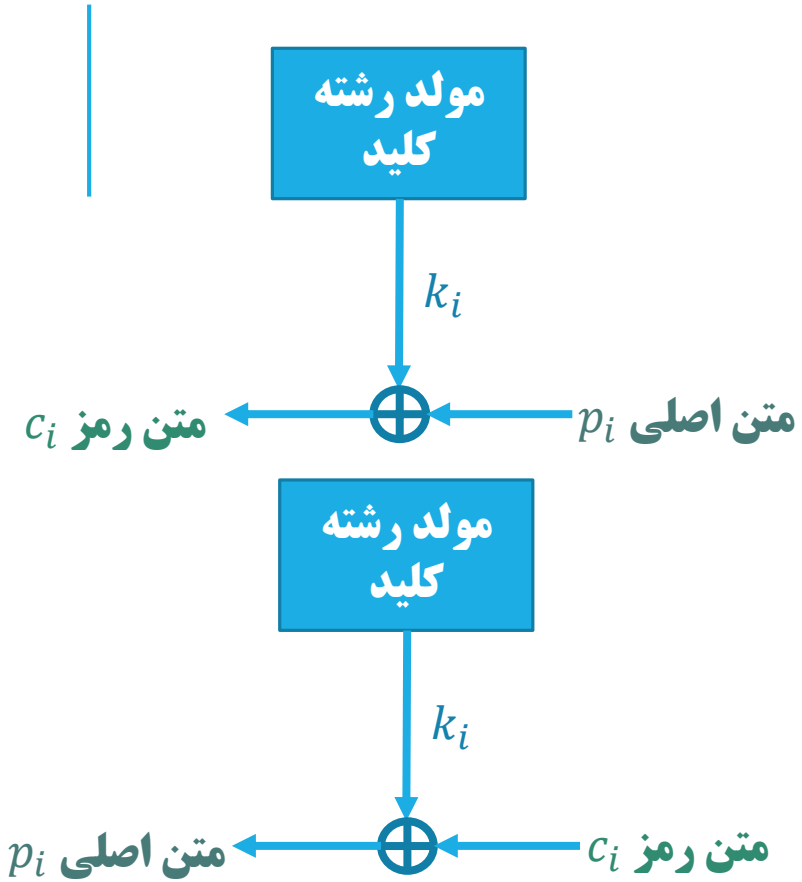
https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

روش رمزهای سنتی

- سیستم کلیدخودکار
  - طول کلید برابر متن برای جلوگیری از تکرار
  - باز خطرپذیر
  - ادعای غیرممکنی در مقاله ۱۹۱۷ ساینتیفیک امریکن
  - به طریق اولی درباره رمزهای جدیدتر

https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

روش رمزهای سنتی- ورنام



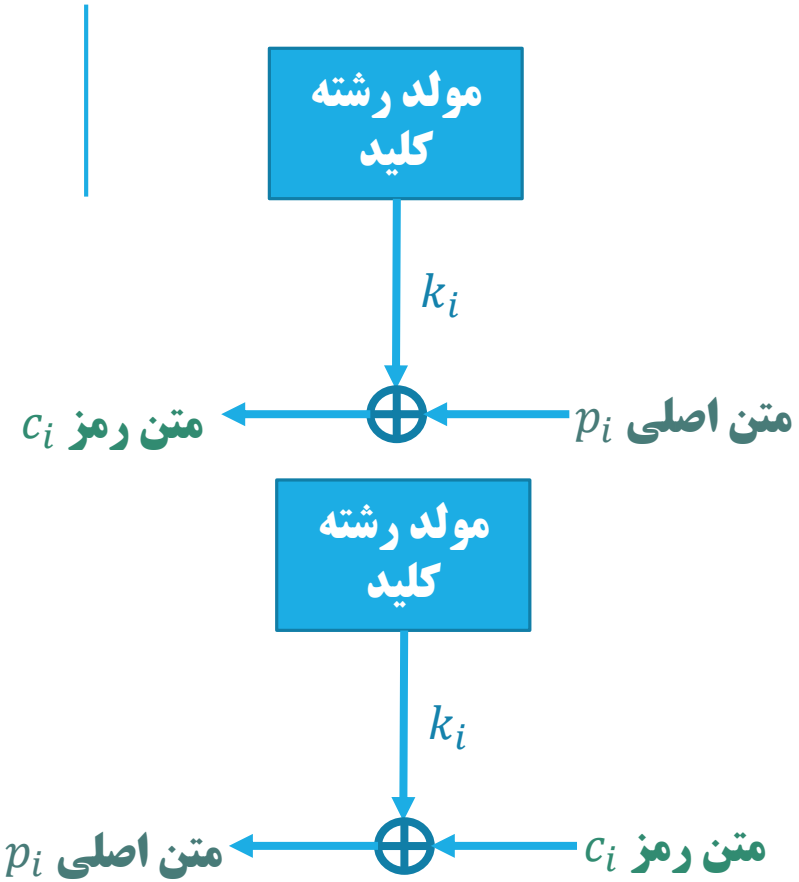
- گلیبرت ورنام مهندسی در آت و ت
  - ۱۲۹۷ شمسی
- رمز ورنام-
  - طول کلید برابر متن‌اصلی
  - بدون ارتباط آماری با متن اصلی
- رمزگذاری

$$c_i = p_i \oplus k_i$$

  - p_i- عدد i-اُم دودوئی متن اصلی
  - k_i- عدد i-اُم دودوئی کلید
  - c_i- عدد i-اُم دودوئی متن رمز
  - $\oplus$- عملوند یاانحصاری
  - مقایسه با معادلهٔ ویژنه؟
- رمزگشائی
  - به دلیل خاصیت یاانحصاری

$$p_i = c_i \oplus k_i$$

روش رمزهای سنتی- ورنام



- امن‌تر از ویژنه
- دودوئی
- اساس و جوهر روش
  - تولید کلید
  - پینشهاد ورنام- اجرای حلقه‌ای که در نهایت کلید را تکرار می‌کرد
  - باز احتمال شکست

روش رمزهای سنتی- لاگذاری تک‌بار

- افسر رمز جوزف ماوبرگنه
- طول کلید برابر طول متن اصلی
- کلیدی حاصل از تولید تصادفی از الفبا
- استفاده یکباره از کلید
- امنیت کامل
  - مشکل عملی تولید چنین کلیدهای طولانی
  - توزیع و حفاظت کلید
- کاربرد محدود
- صرفا برای کانال‌های پهنای باند پایین نیازمند امنیت بسیار بالا
- تنها سیستم رمز دارای «مخفی‌کاری کامل»
  - Perfect secrecy
  - حدیث حالات و مقامات کلود شانون

One-Time Pad

روش‌رمزهای سنتی- روش‌های جابجائی

جایگشت حروف متن اصلی

ساده‌ترین

- رمز زیگزاگ- توری راه‌آهن rail fence

m e m a t r h t g p r y
e t e f e t e o a a t

MEMATRHTGPRYETEFETEOAAT

ن		ر		ر		س		ل		د		ب
	ک		ا		ف		ا		ک		ع	

ب‌دل‌س‌ررن‌ع‌ک‌اف‌اک

- ساده جهت تحلیل رمز

روش‌رمزهای سنتی- روش‌های جابجائی

نوشتن پیام در قالب مستطیل درحالت ردیفی و خواندن ستونی آن با جایگشت روی ستون‌ها

کلید	۷	۶	۵	۲	۱	۳	۴
متن اصلی	p	k	c	a	t	t	a
	e	n	o	p	t	s	o
	t	l	i	t	n	u	d
	z	y	x	m	a	o	w

متن رمز ttnaapptmtsuoaodwcoixpetz

- دارای بسامد یکسان
  - ریختن در ماتریس و بازی با با محل ستون‌ها
- راه‌حل؟
  - استفاده از جدول‌های بسامد جفت‌گرم‌ها و سه‌گرم‌ها
  - افزودن پیچیدگی با بیش از یک بار جابجائی
  - تمرین

ماشین‌های چرخان

استفاده از چند مرحله رمزگذاری

- طراحی الگوریتمی با تحلیل رمز مشکل‌تر
- صادق برای هر دوی انواع جانشینی و جابجائی

مهم‌ترین نمونهٔ پیش از «ارد»

- ماشین‌های چرخان
  - انیگمای آلمانی و پرپل ژاپنی در جنگ دوم
  - ادعای شکستن آنها
  - عاملی مهم در پیروزی متفقین

Rotor Machines

ماشین‌های چرخان

ابزاری الکترومکانیکی

- اختراع مستقل
- ابتدا در ۱۲۹۳ شمسی

انتخاب خروجی با ورود هر نویسه

رمزگذاری

- تقریب ذهن: رمز جانشینی ساده
  - در صورت سیم‌بندی بدون چرخندگی
  - نگاشت هر کلید ورودی به نویسه‌ای خروجی
- مثال- با کلیک حرف k، تولید حرف C
  - قاعده جانشینی ساده

Rotor Machines

ماشین‌های چرخان

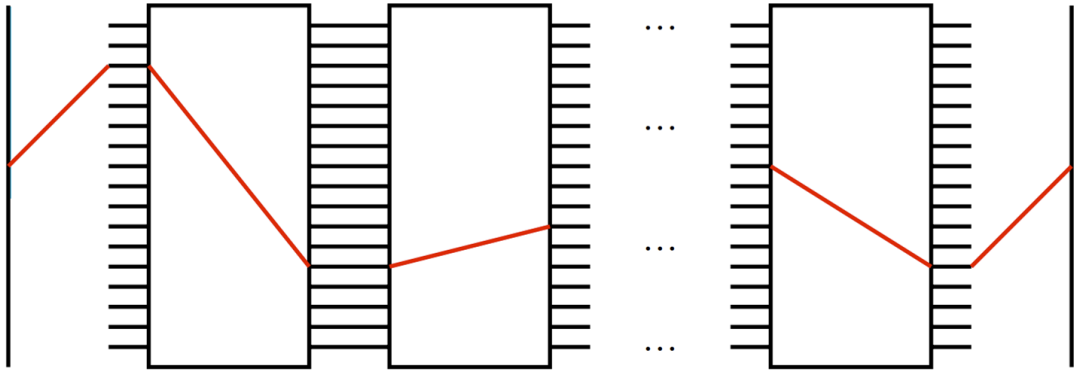
افزودن چرخ
- ماشین جانشینی ساده
- افزودن چرخ با سیم‌بندی
- چرخیدن چرخ با دنده پس از هر کلیک

در نتیجه پس از کلیک دوباره حرف، کدی متفاوت به دلیل سیم‌بندی داخلی
- مثال- کلیک KK در صفحه کلید تولید CB به دلیل چرخیدن پس از هر کلیک

نیاز به مخفی ماندن سیم‌بندی داخلی چرخ
- کشف در طول زمان

جهت کشف متن رمز
- نیاز به ماشینی با همان چرخ

افزودن چرخ موجب قوی‌تر شدن رمز چند جانشینه



ماشین‌های چرخان

پیچیده‌ترسازی جهت بهبود امنیت

- افزودن چرخ‌های بیشتر
  - تحویل خروجی هر چرخ به ورودی چرخ بعدی
- به طریق اولی اتصال خروجی چرخ دوم به ورودی چرخ سوم و تداوم این عمل به تعداد چرخ‌ها

عوامل استحکام رمزنگاری

- تعداد چرخ‌ها
- اندازهٔ هر چرخ
- تعداد نوع‌های چرخ (با سیم‌بندی متفاوت)

هر چرخ دارای سیم‌بندی داخلی متفاوت

- لزوم مخفی ماندن جانشینی هر چرخ از دشمن

جهت مشکل کردن تحلیل رمز و همچنین اطمینان از تغییر سیم‌بندی چرخ با بسامدهای متفاوت

- چرخش با سرعت متفاوت هر چرخ
- فرضا با چرخش ۲۶ یا ۳۲ حرفی چرخ اول، چرخ دوم یک حرف بچرخد.

رمز متقارن

- به معنای رمز کردن متن رمز موجب تولید متن اصلی

Rotor Machines

پنهان‌نگاری (استگانوگرافی)

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told. by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16t proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

پنهان‌سازی وجود پیام

- خواندن حروف خاص در متن
- جوهر نامرئی
- برجستگی بعضی حرف‌ها
- نورمرئی

Myers, L. *Spycomm: Covert Communication Techniques of the Underground.* Boulder, CO: Paladin Press, 1991.

منابع

[شنون]

[استالینگز۱۷]

[س ل ر س] فصل ۳۱

http://www.crypto-it.net/eng/simple/rotor-machines.html