Date: ۱۴۰۰/۷/۶ ۹۷۵۲۱۰۱۸ رامتین احسانی Subject: یادداشت کلاسی

*

سنتی	آنیگما	مدرن	نامتقارن
	1948	1976	

فعلا در حال بررسی این ها هستیم

* جانشینی چند حرفی ← بنظر می رسد قوی تر از تک حرفی باشد.

* حملات فرکانسی ← متن ← هر کاراکتر چند بار تکرار شده است

تعداد بالا ← a یا b یا ... کم ← x یا z یا w ...

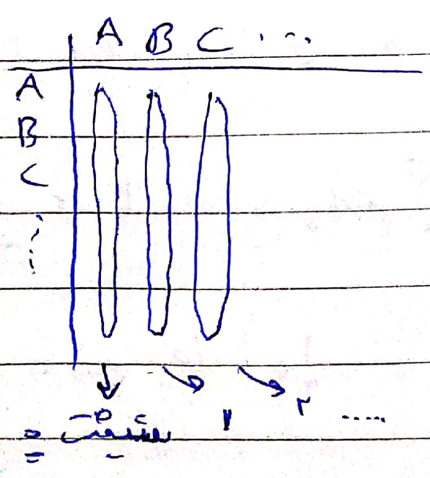
← تک حرفی را تبدیل می کردند ← چند حرفی

* هوموفونیک ← برای حروف با فرکانس بالا ← جایگزین با چند حرف

a یا e یا ... ها

* الگوریتم ویگنر ← چند الفبایی

← نیاز به جدول داریم



باید کاملا محرمانه باشند ← کلید

مثال ← BAND

Date: / /

Subject:

* مثال ← کلید BAND

This is an example

BAND BANDBAND BAN

UH .....

تطابق این ← اولین حرف پیام T

کلید ∿ ∿ B

دو حرف

در جدول

A, H → H ← U

* ویژگی خاص ← { کلید اول ← V
کلید دوم ← S

← چند الفبایی

یک حرف ← X یکتا X

با این حال حتی این الگوریتم هم شکسته شده است.

* فضای کلید ← 26^d طول کلید = d

← قدرتمند تر از سزار و مستوی

* جایگشتی ← ترتیب را بهم می‌زنیم ← در کل تغییری نمی‌کند

انتخاب طول ← بعد از آن حروف را بهم بریزیم.

به چیزی احتیاج داریم؟ ← طول (کلید) + نحوه بهم زدن

فضا ← طول! ← مثلاً $20!$ طول

Date: / / Subject:

* حفظ کردن مثلاً ۲۰ عدد خیلی سخت است ← کلید ها باید کوتاه تر شوند

- یک عدد مانند ۷ ← یک جدول با ۷ ستون

به صورت ستونی رمزگذاری ← وارد کردن واژه ها به صورت ردیفی کنیم

این روش به صورت ستونی و ردیفی (برعکس) هم می تواند باشد

* نهان نگاری ← پنهان کردن یک پیام داخل یک پیام دیگر ← تصویر، ویدیو، پیام، ...

- نهان نگاری ← هدف عکس نهان نگاری را دارد

Steganography

نوشتن پنهان

پنهان کردن پیام های مخفی داخل پیام ها

* رمزنگاری ← مخفی سازی محتوای پیام

نهان نگاری ← مخفی سازی وجود پیام

* یکی از روش های نهان نگاری عکس ← یک پیکسل ← RGB

پنهان سازی ← برای همه این کار ← بیت های آخر هر کدام را تغییری دهیم

از کاری می کنیم

Date: / /

Subject:

* نشان گذاری ← water marking

* تفاوت با نهان نگاری؟ ← در نشان گذاری کسی متوجه وجود پیام نمیشود

برای ما اهمیتی ندارد

* نشان گذاری ←
  - Visible / Invisible
  - شکننده / غیر شکننده