Date: ۱۴۰۰/۸/۹ Subject: یادداشت کلاسی رامتین احسانی ۹۷۵۲۱۰۱۸

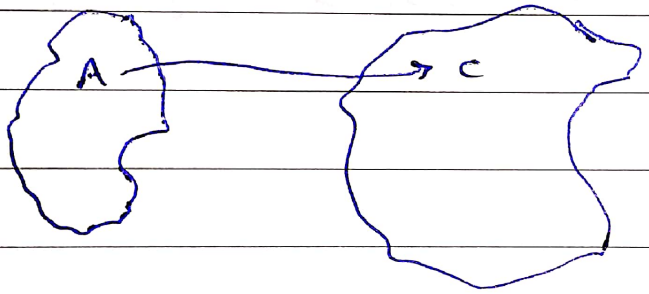
* پیشنهاد شانون ← استفاده از ترکیب جانشینی و جایگشت

* گمراه کنندگی ← رابطه بین متن رمز و کلید تا حد امکان پیچیده باشد

← confusion

* انتشار ← ساختار آماری متن آشکار بر روی حجم وسیعی از متن های رمز شده ممکن پراکنده گردد ← diffusion

plain Text.



cipher Text

A یکبار C شود
A دو بار B شود
⋮
← به احتمال مساوی و بی‌وقفه منتشر شود

* الگوریتم کلید متقارن ← Performance بالا

← هم‌آیین، هم‌باب کلید را داشته باشند

* همه الگوریتم‌های رمزنگاری قبل از ۱۹۷۰ ← کلید متقارن

* مشکل ؟ ← انتقال کلید

* کلید متقارن ← بلوکی ← Block cipher

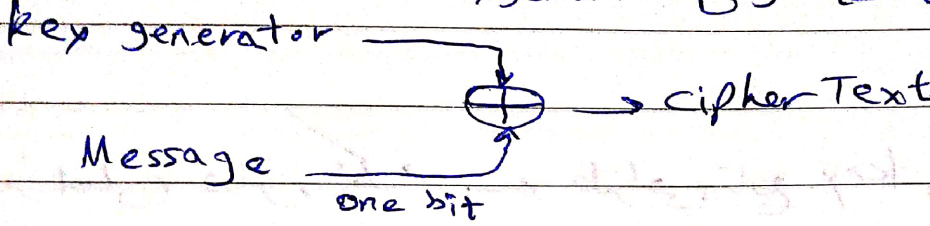
← جویباری ← Stream cipher

Date: / / Subject:

* stream ← یک بیت از مسج

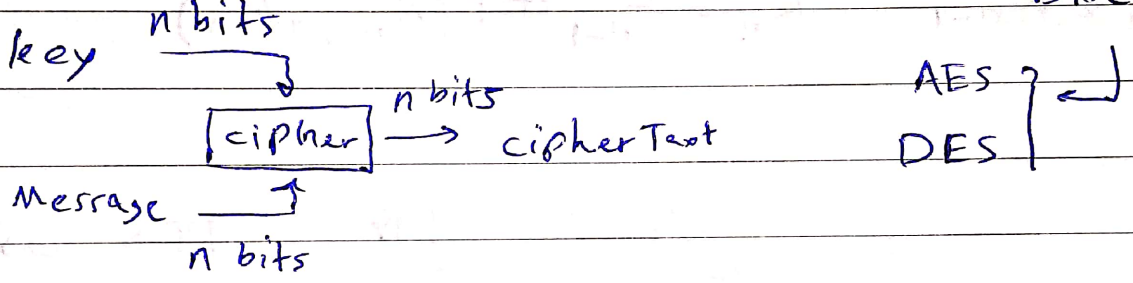
cipherText ← XOR ← یک بیت از کلید

کلید داستان ← طراحی keygenerator



* decrypt ؟ ← باز هم XOR

* Block



* مثالی از جویباری ← الگوریتم f8 ← تولید کننده کلید در شبکه های تلفن همراه ← ورودی ← ck ← ۱۲۸ bit

* بلوکی ایده آل ← به صورت جایشینی کامل با طول n بیت

نوع رمز ← ۲۴ ← This is an example

* بلوکی ← خیلی ها مبنی ← شبکه های فایستل Feistel

* یک تعدادی راند ← تقسیم متن ← Right , left

این دستورالعمل ها

* در هر راند ← جای Right , left عوض می شود

* هسته اصلی در این شبکه ← طراحی تابع $\underline{F}$ ، $\underline{key}$

* فرمول‌ها:

$$L_n = R_{n-1} \qquad R_n = L_{n-1} \oplus F(R_{n-1}, k_n)$$

* در DES ← ۱۶ بار راند داریم