

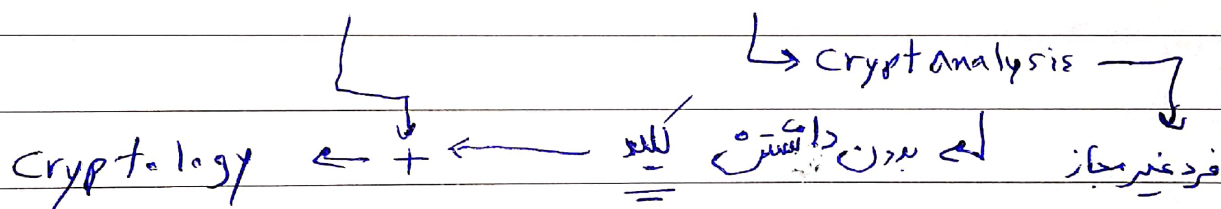
* Eve در صورت داشتن ک می تواند به متن اصلی برسد؟

که یا کارش سخت است؟

* Cyphering = الگوریتم تبدیل متن اصلی به متن رمز

* Encryption = کل فرایند

* علم اصول و روش های رمزنگاری در مقابل Cryptography



* ۲۴ کلید = در کل در گزار می توانیم داشته باشیم

لکه کل فضا = طول کلید = $\log_2 24 = 4.7 \text{ bit}$
 $\log_2 24 = 4.7 \text{ bit}$

* رمز پیچیده تر = مستوی (Affine)

$$E_k(m) = (a \times m + k) \bmod 26$$

سزار $\rightarrow a=1$

* هر چه کلید بیشتر = سخت تر

brute force * امتحان کردن تمام حالت ها = هوشمندانه نیست

برای شکستن رمز

کوچکتر کردن فضا

الگوریتم هوشمندانه تر

* در الگوریتم مسدود، a چه عددی می تواند باشد؟

$$m = \{0, 1, 2, \dots, 2^a\} \quad a=2, \quad k=1$$

نکات دیگر: a نیست x \rightarrow $2 \xrightarrow{map} a$
 $15 \rightarrow a$
 a باید مثبت به 2^a اول باشد

که k مقصود نیست $\leftarrow a$ اشتباه است

کلید $= 2^4 \times 12 \rightarrow 2^4$ حالت $k = 12$ حالت

که عدد کلید $= 11, 28 \text{ bit}$
 $\log_2 12 =$

* مجموعه کلید \leftarrow نکات کلی \leftarrow نکات تصادفی

که به سطر a یک به یک بودن

و پوشا بودن

$\rightarrow 2^4! = 2^{11,6} \approx 11 \text{ bit}$

Date: / /

Subject:

* چرا همیشه از تصادفی استفاده کنیم؟

لے Cost سیستم دائماً در حال

بجیده تر شدن است

مشکلات امنیتی → نگهداری کلید سخت است →

* الگوریتم های جانشینی

لے یک حرف یا حید حرف سے پہ چای آن ہا ہے یک یا حید حرف دیگر

سزار → تک حرفی ہا

یک حرف دیگر → Th → چند حرفی ہا