Date: ۱۴۰۰/۷/۴ ۹۷۵۲۱۰۱۸ راستین احسانی Subject: یادداشت کلاسی

* Eve در صورت داشتن چه چیزی می‌تواند به متن اصلی برسد؟ کلید یا کاپی سخت است؟

* cyphering ← الگوریتم تبدیل متن اصلی به متن رمز
  * encryption ← کل فرآیند
* علم اصول و روش‌های رمزنگاری در مقابل cryptography
  - cryptanalysis ← فرد غیرمجاز ← بدون داشتن کلید
  - cryptology ← +

* ۲۶ کلید ← دزل در سزار می‌توانیم داشته باشیم
  - کل فضا ← طول کلید ← $\log_2 26 = 4.7$ bit
    - ≈ 5 bit

* رمز پیچیده‌تر ← مستوی (Affine)
  - $E_k(m) = (a \times m + k) \bmod 26$
    - سزار ← if $a = 1$

* هر چه کلید بیشتر ← سخت‌تر

Date: / / Subject:

* brute force ← امتحان کردن تمام حالت ها ← هوشمندانه نیست

برای شکستن رمز ها

کوچک‌تر کردن فضا ها

الگوریتم هوشمندانه‌تر ←

* در الگوریتم مستوی، a چه مقدی می‌تواند باشد؟

$m = ۲۰, ۱, ۲, \dots, ۲۵$؟ $a = ۲$, $k = ۱$

$۲ \xrightarrow{mod ۲۶} ۵$

$۱۵ \rightarrow ۵$

← نگاشت یک به یک نیست ✗

a باید نسبت به ۲۶ اول باشد

k مقدار نیست ← a اشتباه است

۱۲ حالت $k =$ ۲۶ حالت → $۱۲ \times ۲۶ =$ کلید

$\log_2^{۳۱۲} =$ ۸٫۲۸ bit ← طول کلید

* مجموعه کلی ← نگاشت کلی ← نگاشت تصادفی

← به شرط یک به یک بودن و پوشا بودن

$۲۶!_{۰} = ۲^{۸۸٫۴} \simeq ۸۸$ bit

Date: / / Subject: .....

* چرا همیشه از تصادفی استفاده نکنیم؟

↳ cost ← سیستم دائماً درحال پیچیده‌تر شدن است

مشکلات امنیتی ← نگهداری کلید سخت است

* الگوریتم‌های جانشینی

↳ یک حرف یا چند حرف به جای آن‌ها یک یا چند حرف دیگر

ساز ← تک‌حرفی

Th ← چند حرفی

یک حرف دیگر ←