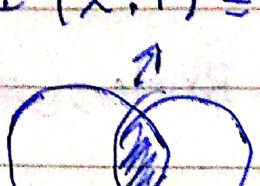
Date: ۱۴۰۰/۸/۴ راتین احسانی ۹۷۵۲۱۰۱۸ Subject: یادداشت کلاسی

* یک سامانه کامل امن است اگر

plaintext ← ciphertext

$I(X;Y) = 0 \iff X \perp Y$



یعنی طور کامل از هم مستقل باشند

* قضیه ۱ ← در یک سامانه امن کامل

← حتما ← $H(X) \leq H(K)$

← امن کامل ← نباشد ←

نیست

$H(X,K|Y)$ *

$H(X) = H(X|Y)$ → $H(X|Y) \leq$

$H(X) \leq H(X,K)$

← چون ۲ فرض داده شده

* قضیه ۲ ← سامانه one Time pad یک سامانه امن کامل است.

* اگر اندازه کلید از متن کوچکتر ← ناامن

This is an example → encryption → cipher

↑ key

← $H(K) = 15 \times \log_2 26$

پس باید کلید طولی بزرگتر یا مساوی ۱۵ داشته باشد تا امن باشد

Date: / / Subject:

* امن کامل ← بهترین شرایط ← هیچ الگوریتمی وجود ندارد که بتواند بهتر از Brute عمل کند.

* محاسباتی ← روشی بهتر از Brute وجود دارد.

* یک رمزنده OneTime باید cipher را با کلید XOR کند تا به Plain برسد.

← مشکل امنیتی ← تولید کلید ← رندوم کامل

↳ NLFSR

* فاصله قابل شکست:

← unity distance

← حداقل طول بیتی که باید در اختیار شما قرار بدهم که

↳ $H(K|Y_1, Y_2, \dots Y_n) = 0$

↳ با Y_1 تا Y_n کلید را بیابیم

هرچه unity بیشتر ← سیستم امن‌تر است

* معیارهای پنج گانه

- میزان امنیت
- اندازه کلید ← حتی‌المقدور کوتاه و ساده
- انتشار خطا
- بسط یا گسترش پیام
- پیچیدگی کم در روند ساده encryption و decryption