جلسه ۲

آنتروپی ← نقاشی بی‌نظمی سیستم

کاملاً رندوم = توزیع کاملاً یونیفرمت ← ایده‌آل ما است. ← در غیر این صورت دشمن راحت می‌تواند کلید را حدس بزند

دلیل اینکه طول کلید باید برابر متن باشد ← نباید reuse شود.

کاربرد OTP ← وقتی دو نفر خیلی اطلاعات مهمی دارند و می‌خواهند با هم در ارتباط باشند ← عملاً خیلی کاربرد ندارد.

مدیریت کلید سخت ← داشتن نیاز آفلاین و share کردن کلید بین n نفر

Diffusion: دشمن با دیدن متن رمزشده نتواند به متن اصلی برسد.

permutation ① جابه‌جایی

substitution ② جایگزینی

Confusion: ... نتواند رابطه اش با کلید را بیابد.

هر الگوریتم تصادفی؟

تصادفی ← K → [PRG] → خروجی شبه‌تصادفی : 2^n L یک دوره تناوب دارد ← در دوباره تکرار می‌شود.

← پس دوره تناوب باید بزرگ باشد.

RC4

توضیح کد:

S [0|1|2|....|255] → هر خانه یک بایت است

طول کلید؟ گرفتن توانایی حمله search کامل از دشمن ← ۱۲۸ (مینیمم)

در roundها لازم است permutation و substitution انجام شوند ← برای هر round یک کلید یکتا داریم. (تیپس)

در یک block cipher ایده‌آل انتظار داریم برای یک ورودی L بیتی تعداد حالات محتمل خروجی چند تا باشد؟ 2^L

جلسه ۵:

تابع R باید چه خصوصیتی داشته باشد؟ هر ورودی به یک خروجی برود (یک به یک باشد) - برای بستن به کلید از ورودی نباید به سادگی برگشت‌پذیر باشد. (فرض ساده داشته باشد ولی برگشت سخت باشد)

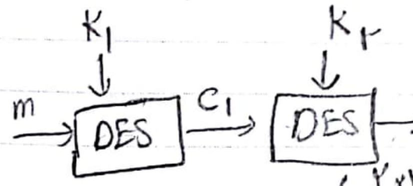
ساختار اصلی در block cipher: feistel، SPN

تابع f نیز مانند R باید ویژگی‌های آن را داشته باشد ← در Feistel ← یک تغییر در ورودی کاملاً در خروجی پخش است. با جایگشت و جایگزینی کار دهد

← confusion ← جایی که تابع f اعمال می‌شود diffusion ← جابه‌جایی‌ها و همان پخش شدن بیت‌ها

چرا NSA در طراحی اولیه که طول کلید ۱۱۲ بود، آن را ۵۶ کرد؟ قدرتی که در تعقیب خودش می‌تواند طول کلید ۵۶ را سریع حل می‌کند.

- حمله عملی یعنی چه؟ یعنی حمله‌ای که خیلی بهتر از حمله جستجوی کامل باشد ← order زیاد



بهبود DES ← تکرار DES

2DES ← meet in the middle attack ← فضای search را 2^{57} می‌کند. ($2 \times 2^{56} = 2^{57}$) ← طول کلید مؤثر

3DES ← دو نوع دارد که در جزوه است.

$$3DES2_{K_1 \| K_2}(M) = DES_{K_2}(DES^{-1}_{K_1}(DES_{K_2}(M)))$$

← طول کلید؟ ۱۱۲

در تا ۵۶ را کار هم می‌گذارد که می‌شود ۱۱۲ تا

$$3DES_{K_1 \| K_2 \| K_3}(M)$$

یکی از کلیدها چون می‌تواند Meet in the middle انجام شود ← ماهیت خود را از دست می‌دهد