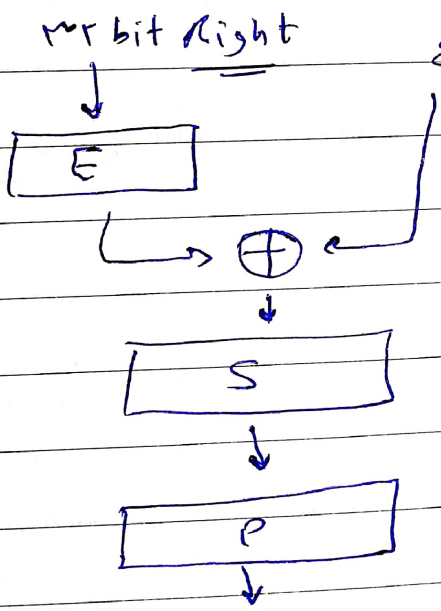
Date: ۱۴۰۰/۸/۱۶ یادداشت کلاسی Subject: راشین احسانی ۹۷۵۲۱۰۱۸

* DES ← آمریکایی
  - ← Backdoor به لو نادن محتویات رو ← شک بر وجود
  - ← مبتنی بر فایستل
  - ← ۱۶ راند ← هنوزم خیلی ازش نمی‌دونیم ← با مهندسی معکوس چیزایی فهمیدیم
  - ← ورودی هر دور ← ۶۴ بیت
    - ← ۳۲ بیت راست
    - ← ۳۲ بیت چپ
  - طول کلید ← ۶۴ bit

* تابع F




E → expand → 32 → 48 bit

* تنها جایی که می‌تونیم سیستم رو از حالت خطی خارج کنیم ← تابع F ← عنصر خطی → خطی

* در DES ← ۶۴ بیت کلید ← ولی قدرت ۵۶ بیت
  - ← ۸ بیت → Parity → هدر
  - قدرت → $2^{56}$

* ۸ تا Sbox ← عنصر خطی می‌کنند

Date: / /  Subject:

* هرکدام از S های ۶ بیت ورودی
  ← ویژگی confusion ← جانشینی

* P ← جایگشتی
  ← diffusion

* حملات به DES ← راهکار موقت
  ← استفاده از چندین بلوک DES
    ↳ 3DES

* چالش الگوریتم متقارن ←
  ① تبادل کلید
  ② توافق کلید
  ← سازوکارهای برقراری کلید
    ↳ key establishment

معمولاً کانال انتقال امن است
؟
① key transport ← یک سمت کلید را تولید کرده و انتقال می دهد.

② key agreement ← هر دو سمت در فرآیند تولید مشارکت می کنند.
  ← آلیس ← A ← می فرستد به باب
  باب ← B ← می فرستد به آلیس
  ← کلید ← AB
  ← نرمال می کنیم فعلا
    ↳ Secure channel

Date: / /  Subject:

* خیلی وقت ها ما کانال امن نداریم

- الگوریتم های کلید نامتقارن

- ElGamal
- RSA
- Diffie-Hellman

} که از ۱۹۷۶ به انقلاب بعدی به

* یک کلید X به صورت یک جفت کلید

Publickey عمومی
Privaite key محرمانه

* عمومی به همه می دهند  $E_{ke}(X)$ ← Alice

* محرمانه پیام به رمز کردن با کلید عمومی

- باز کردن با کلید محرمانه

Bob ← $D_{K_d}(Y)$

* همه ی علم کلید نامتقارن به وابسته به تئوری اعداد