Date: ۱۴۰۰/۸/۳۰

یادداشت کلاسی Subject: رامتین احسانی ۹۷۵۲۱۰۱۸

* دیفی هلمن ← قدم اول ← انتخاب عدد اول ← مثل P = ۱۳

↳ مولد ← G = ۴

← ریشه اولیه

مجموعه کاهش یافته در باقیمانده‌ها

مثلا ← برای ۵ ← {۱،۲،۳،۴}

← ادعا می‌کنیم ۲ ریشه اولیه است ← ۲ را به توان همه اعضا می‌رسانیم و mod ۵ می‌گیریم

→ {۲،۴،۳،۱} ← همان مجموعه ← ✓

ولی با جایگشت

بعد از مشخص شدن P و G ← انتخاب Private در هر دو طرف

↳ بعد از محاسبات ← هر دو به $(g^B)^A$ می‌رسند

↳ کلید مشترک

* مشکل ← حمله مرد میانی ← g^A را از آلیس می‌گیرد

↳ عدد دیگری تولید می‌کند ← g^C ← به باب می‌فرستد

↳ g^B را از باب می‌گیرد

↳ g^D را به آلیس می‌دهد

↳ آلیس و باب با مرد میانی کلید مشترک دارند

Date: / /

Subject:

* مشکل یا دلیل این حمله ← نبود احراز هویت

له ← باعث حمله مرد میانی

* برای حل احراز هویت ← استفاده از کلید ناسشار و یا متقارن

↓

ایجاد دور

له ← دیفی همان معرفی شده که دیگر

مجبور به استفاده از متقارن یا

ناسشار نباشیم

* Forward Secrecy

له ← آلیس و باب با یه روشی ← secret مشترک رسیده اند

و آن را برای چندسال نگهداری کنند

له ← اگر یک نفر به کلید برسه ← کل اطلاعات لو میره

راهکار ؟ ← کلید را به صورت دوره ای عوض کنیم

له ← برای هر session کلید جدا تولید کنیم

له ← اگر لو برود ، فقط اطلاعات session لو می رود

* اگر به A و B دست پیدا کنند ← امنیت خود سیستم هم

خواندن کلید خصوصی از حافظه ← بسیار مهم است

Date: / /

Subject:

* نیاز به گواهینامه و مرکز صدور گواهینامه داریم ← نهاد سوم

له مشکل حمله ردیابی به سامانه‌های گلد ناستقار ان

*