Date: ۱۴۰۰/۸/۱۸ ۹۷۵۲۱۰۱۸ راستین احسانی Subject: یادداشت کلاسی

★ کلید نامتقارن ← رمزعبوری ← همه می‌توانند رمزگذاری کنند

له رمزخصوصی ← فقط باب می‌تواند رمزگشایی کند

★ هدف از امضای دیجیتال ← احراز هویت

له ذاتاً در کلید متقارن پرد

له به صورت فنی مستر است

فقط آلیس یا ← به خاطر استفاده از ← یک کلید

باب

کلید را دارند

★ برای احراز هویت

له رمزگذاری با کلید خصوصی

له رمزگشایی با کلید عمومی

★ آلیس به باب

authentication هم

له رمز کردن با Private key خودش (آلیس)

له " " Public key طرف مقابل (باب)

★ تعداد کلید در نامتقارن ← $\frac{n \times (n-1)}{2}$

★ در نامتقارن ← نیاز به کانال امن؟ ← اطمینان از اینکه کلید عمومی متعلق به شخص خاصی هست یا نه

★ برای اطمینان از هویت کلید عمومی ← ایجاد certificate

↳ نهاد سوم

↳ CA

★ سرعت عمل پایین تر الگوریتم‌های نامتقارن نسبت به متقارن

★ الگوریتم‌های کلید متقارن در توزیع کلید نقش مشکل دارند.

★ امنیت الگوریتم‌های کلید نامتقارن ← وابسته به نظریه اعداد

↳ مبتنی بر مدول کلید

★

مجموعه کامل باقی‌مانده‌ها در هنگ $n=4$ ← مجموعه $\{0,1,2,3\}$

$\{1,2,3,4\}$

همواره دارای n عضو

$\{-1,0,1,2\}$

★ تنها مجموعه کامل باقی‌مانده‌ها اعضای مثبت و کوچکتر از n

$\{0,1,2,3,\dots,n-1\}$

Date: / /

Subject:

* مجموعه کاهش یافته مانده‌ها ← زیرمجموعه از مجموعه کامل مانده‌ها

↓

$(r_i, n) = 1$

↓

$\{0, 1, \dots, n-1\}$

* تعداد عناصر مجموعه کاهش یافته مانده‌ها ← تابع اویلر ← $\varphi(n)$

* برای اعداد اول ← مثلاً ← ۱۳ ← $\varphi(n) = n-1$