Date: ۱۴۰۰/۸/۲۵ ۹۷۵۲۱۰۱۸ راتین احسانی Subject: یادداشت کلاسی

$n = pq$ ★ $c = m^e \pmod n$

$0 \le m < N$ ← اگر m نسبت به n اول نباشد چی؟

↳ $(m,n) = p$ or q

↳ احتمال این رخداد خیلی کمه

★ $n = pq$ ← p و q نباید باهم برابر بشوند

★ مثال:

$p = 3$
$q = 11$ $\rightarrow n = 3 \times 11 = 33$

$\varphi(n) = (3-1)(11-1) = 20$

$\begin{cases} e < \varphi(n) \\ (e, \varphi(n)) = 1 \end{cases} \rightarrow e = 7$

$ed \equiv 1 \pmod{20} \rightarrow 7d \equiv 1 \pmod{20}$

↳ $d = 3$

↳ 3 و 11 را نباید پخش کنیم ← n را باید بدهیم

↳ 33

e را هم باید پخش کنیم

Date: / / Subject:

★

$\varphi = 20$
$n = 33$
$e = 7$
$d = 3$
$p = 3$
$q = 11$

$m = 2$

$\rightarrow C = m^{e} \pmod{n} = 2^{7} \pmod{33} = 29$

$m = C^{d} \bmod n = 29^{3} \bmod 33 = 2$

★ مشکل نامتقارن ← روشی توزیع کلید

← بسیار سخت

← استفاده از HSM ← Hardware Security Module

← رمزگذاری
امضای دیجیتال ← رمز با کلید خصوصی باز کردن با کلید عمومی
تبادل کلید

★ پروتکل تبادل کلید دیفی - هلمن

← 1976
← تحولی بزرگ در رمزنگاری نامتقارن
← فقط توافق کلید بهتر است

مسأله بسیار سخت

$a^{x} = b$ ← مسأله لگاریتم گسسته

NOTEBOOK iman

Date: / /

Subject:

* دیفی-هلمن مبتنی بر لگاریتم گسسته

* که توافق بر P و G به روی اولیه عدد P

که مثال P = ۱۳ G = ۶

که آلیس و باب هردو می دانند

آلیس که تولید پارامتر محرمانه Private = ۵

باب که Private = ۴

$۶^۵ \bmod ۱۳ = ۲ \rightarrow$ Public

که می فرستد به باب

$۶^۴ \bmod ۱۳ = ۹$

که می فرستد به آلیس Public

$۹^۵ \bmod ۱۳ = ۳$

$۲^۴ \bmod ۱۳ = ۳$

shared secret

shared secret