مبانی رایانش امن
رمزنگاری- روش‌های نامتقارن

محسن هوشمند
دانشکده تکنولوژی اطلاعات و علم رایانه
دانشگاه تحصیلات تکمیلی علوم پایه زنجان

رمزنگاری کلید عمومی(نامتقارن)

توسعهٔ کلید عمومی یا نامتقارن

- محتملا بزرگترین و شاید تنها انقلاب سرتاسر تاریخ رمزنگاری

رمزنگاری از ازمنهٔ قدیم تا دورهٔ معاصر

- ابزارهایی از جنس جانشینی و جایگشت
- سپس ماشین‌های چرخنده
- سپس ارد
- ولی همچنان کار هر دو بر اساس جایگشت و جانشینی

رمزنگاری کلید عمومی(نامتقارن)

رمزنگاری کلید عمومی

- جدایی بزرگی از رمزنگاری
- به جای جایگشت و جانشینی، مبتنی بر تابع‌های ریاضی
- نامتقارن و بر مبنای دو کلید
- تاثیری عمیق دو کلیده بودن بر محرمانگی، توزیع کلید، احراز هویت

عدم تمایز تحلیل‌گر رمز میان شکستن رمزنگاری متقارن و غیرمتقارن

همچنین به دلیل نیاز به محاسبات زیاد، عدم بازنشستگی روش متقارن و همچنان استفاده از آن

اصول دستگاه رمز کلید عمومی

سربرآوردن مفهوم رمزنگاری کلید عمومی از تلاشی برای حمله به دو مشکل سخت مرتبط با رمزنگاری متقارن

- اولین مورد توزیع کلید
  - توزیع کلید متقارن نیاز به داشتن کلید یکسان در دستان دو طرف ارتباط
  - توزیع و ارسال کلید به آنها
  - همچنین نیاز به استفاده از مرکز توزیع کلید
  - نیاز به مرکز ⟸ خود نفی کنندهٔ امر رمزنگاری!
- مشکل دوم امضای دیجیتال

انقلاب مفهومی دیفی و هلمن در سال ۱۳۵۵

- با روشی که هر دو مشکل را پوشش می‌داد

دستگاه رمز کلید عمومی

الگوریتم نامتقارن

- رمزگذاری با یک کلید
- رمزگشائی با کلیدی متفاوت اما مرتبط

مشخصه‌های اصلی چنین الگوریتم‌هائی

- امکان استفاده از هر یک از دو کلید برای رمزگذاری و دیگری به عنوان رمزگشا

شش بخش رمزنگاری کلید عمومی

- متن اصلی- پیام خوانائی است که ورودی الگوریتم است
- الگوریتم رمزگذاری- انجام چند تبدیل را بر متن اصلی بر عهده دارد.
- کلیدهای عمومی و خصوصی- جفتی از کلید که اگر یکی برای رمز بکار رود دیگری برای کشف بکار می‌رود.
- متن رمز- متن کد شده که خروجی الگوریتم است
- الگوریتم رمزگشا- ورودی آن متن رمز و خروجی متن اصلی خواهد بود.

دستگاه رمز کلید عمومی

لزوم استفاده هر کاربر از جفت کلیدی برای رمز و کشف

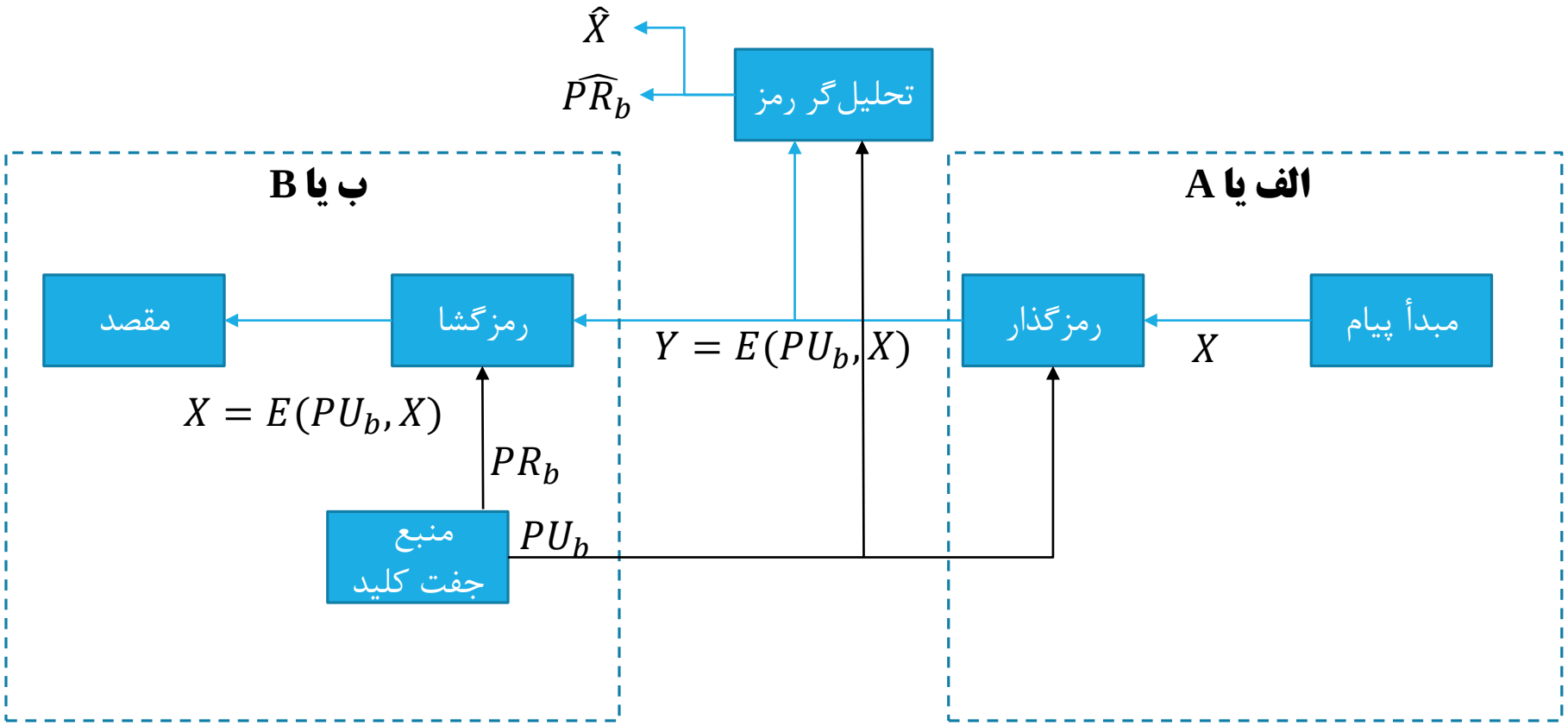
در اختیار عموم گذاشتن یکی از دو کلید
- معروف به کلید عمومی

نزد خود نگه داشتنم کلید دیگر
- کلید خصوصی
- دور از دسترس دیگران

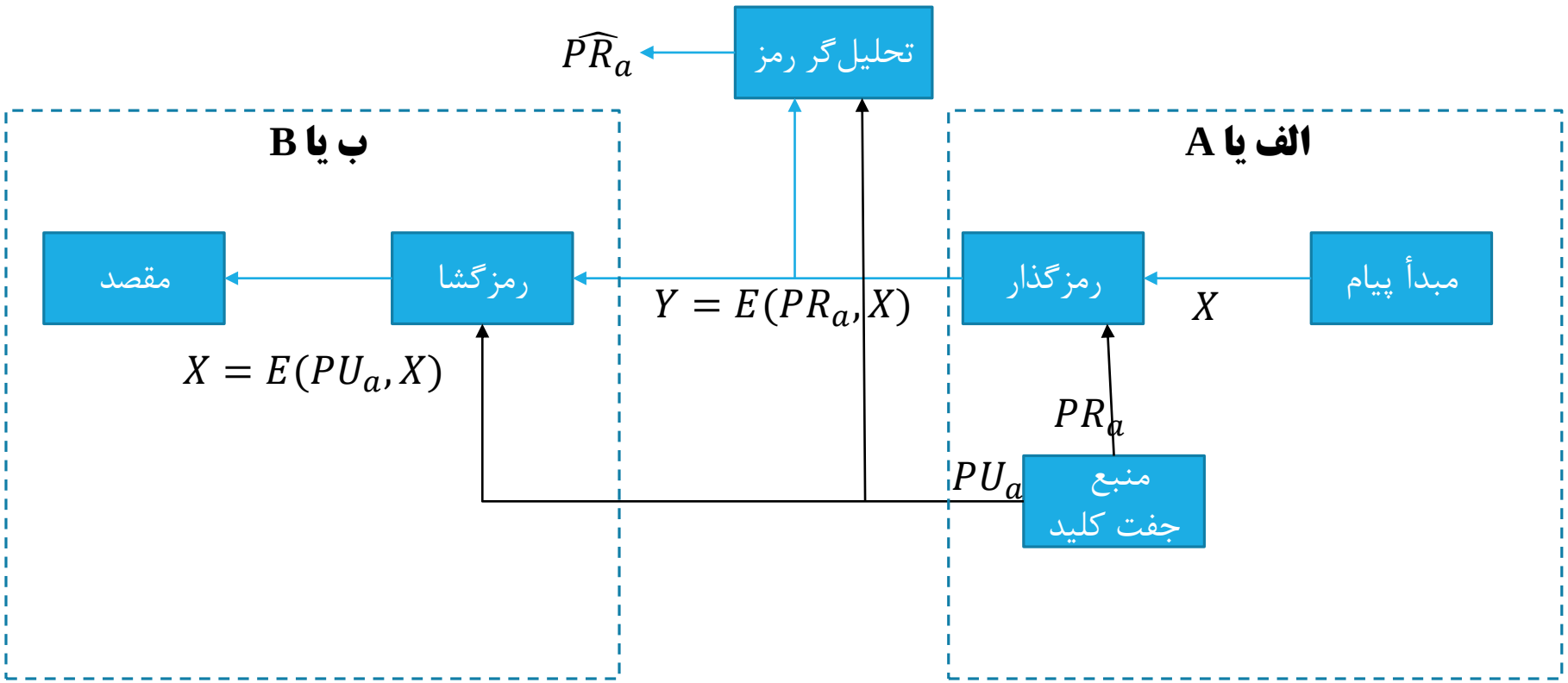
بنابراین دسترسی هر کاربر به کلیدهای عمومی بسیاری از کاربران دیگر

در صورت خواستاری ارسال پیام رمز از الف به ب
- الف متن را با کلید عمومی ب رمز می‌کند
- با دریافت پیام در ب، پیام با کلید خصوصی ب کشف می‌شود.
- هیچ شخص دیگری نمی‌تواند متن را کشف کند
  - به دلیل دراختیار ب بودن کلید خصوصی
  - هر شخصی
    - دارای کلیدهای عمومی تمامی کاربران
    - کلید خصوصی خود .
    - امن بودن اطلاع ورودی تا زمان محرمانه ماندن کلید خصوصی

رمزگذار کلید عمومی- محرمانگی



رمزگذار کلید عمومی- احراز هویت

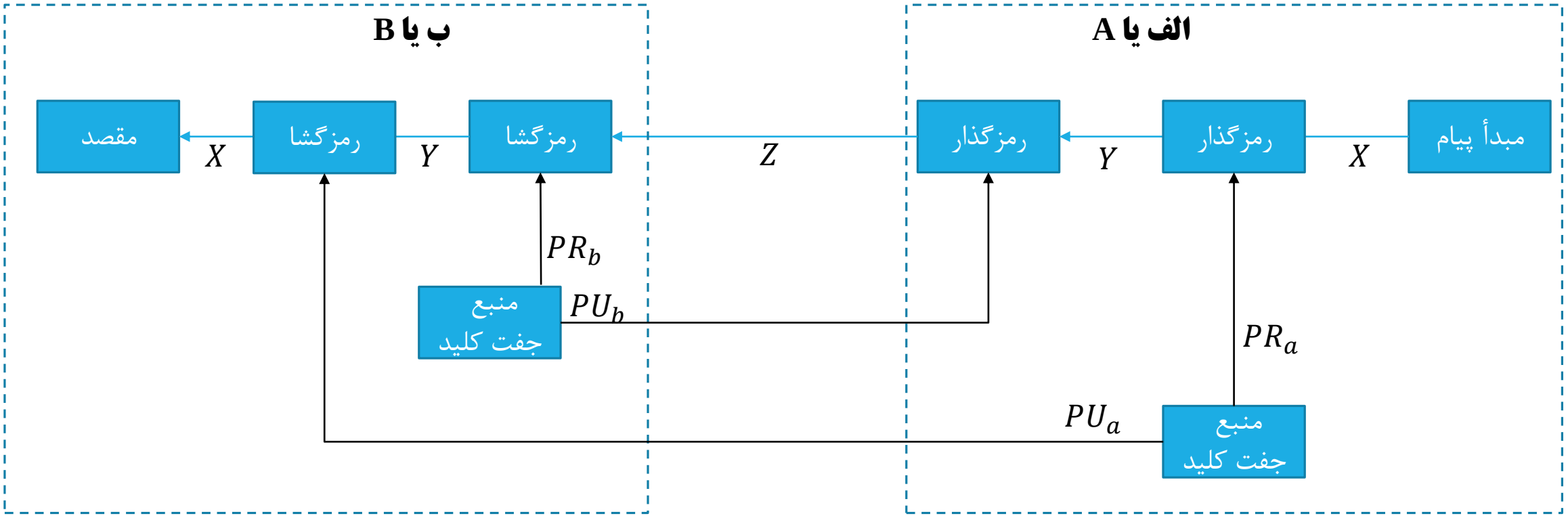


امضای دیجیتال

مورد اخیر فقط جهت محرمانگی نیست

- احراز هویت
- مصون بودن پیام مذکور در طول ارسال از تغییر
  - اما از شنود مصون نیست.
- درصورتی که بخواهیم محرمانگی و احراز هویت را با هم داشته باشیم
  - . از کلید عمومی گیرنده استفاده و پیام و امضا را رمز می‌کنیم.
- بنابراین بسته به هدف از کلید خصوصی فرستنده یا کلید عمومی گیرنده استفاده می‌کنیم.

رمزگذار کلید عمومی- محرمانگی و احراز هویت



کاربردها

سخن کوتاه، کاربردهای دستگاه رمز کلید عمومی

- رمزگذاری/رمزگشائی
  - فرستنده پیام را با کلید عمومی گیرنده رمز می‌کند و گیرنده پیام را با کلید خصوصی خود (گیرنده) کشف می‌کند.

- امضای دیجیتال:
  - فرستنده پیام را کلید خصوصی خود امضا می‌کند.
  - اعمال امضای مذکور با اعمال الگوریتم رمز بر بخش کوچکی از پیام

- تبادل کلید
  - همکاری دو طرف جهت تبادل کلید جلسه
  - به طوری که کلید مخفی رمزنگاری متقارن که برای تراکنش خاصی استفاده دارد و برای مدت کمی معتبر است
  - روش‌های گوناگونی در این دسته

کاربردهای رمزگذار کلید عمومی

جدول زیر انواع روش‌های کلید عمومی و کاربردپذیری هر یک در دسته‌های اشاره شده را مشخص می‌کند.

الگوریتم	رمز/کشف	امضای دیجیتال	تبادل کلید
رسا	بله	بله	بله
خم بیضوی	بله	بله	بله
دیفی-هلمن	خیر	خیر	بله
دی‌اس‌اس	خیر	خیر	بله

چند مفهوم

تابع یک‌طرفه-

- نگاشتی از دامنه به برد
- هر مقدار تابع دارای معکوس منحصر بفرد
- با شرط آسانی محاسبهٔ تابع و نشدنی بودن محاسبه معکوس
- محاسبه مستقیم از کلاس P ولی محاسبهٔ غیرمستقیم سرعتی بیشتر از نسبتی چندجمله‌ای داشته باشد.
- باید توجه داشت حالت میانگین و بدترین حالت پیچیدگی در رمزنگاری کاربردی ندارد.

راحت	$Y = f(X)$
نشدنی	$X = f^{-1}(Y)$

چند مفهوم

تابع یک‌طرفهٔ دررو-

- راحتی محاسبه در یک طرف
- در طرف دیگر نشدنی است مگر با داشتن اطلاعات اضافه
- حل در زمان چندجمله‌ای با اطلاعات اضافه معکوس

راحت، در صورت دانستن X و k	$Y = f_k(X)$
راحت، در صورت دانستن Y و k	$X = f_k^{-1}(Y)$
نشدنی، در صورت دانستن Y و نداستن k	$X = f_k^{-1}(Y)$

سخن کوتاه، ایجاد شمای کلید-عمومی عملی وابسته به کشف تابع یک‌طرفهٔ در-رو مناسب

تحلیل رمز کلید-عمومی

به طریق مشابه، تهدید جستجوی جامع در این نوع رمزنگاری نیز وجود دارد.

- پاتک مقابل این روش مشخص است: انتخاب کلیدهای بزرگ.
- هرچند لازم است به این نکته توجه داشت که رمزنگاری کلید عمومی وابسته به توابع ریاضی معکوس است.
- خطی نبودن پیچیدگی محاسبهٔ چنین روش‌هایی
- نیاز به سبک سنگینی

طول کلید طوری انتخاب شود

- به اندازهٔ کافی بزرگ تا مانع جستجوی جامع و غیرعملی‌کنندهٔ آن
- به اندازهٔ کافی کوچک جهت عملی بودن رمزگذاری و رمزگشائی
- اما در عمل کلیدهایی معرفی شده
  - جستجوی جامع را غیرعملی و در عین حال محاسبه را آنچنان کند کرده است که برای اهداف همه‌منظوری کاربردی ندارد.
- امروزه رمزنگاری کلید-عمومی محدود به مدیریت کلید و کاربردهای امضا شده است.

تحلیل‌رمز کلید-عمومی

نوع حملهٔ دیگر یافتن راهی جهت محاسبهٔ کلید خصوصی با داشتن کلید عمومی است.

- تاکنون اثباتی ریاضی برای امکان‌ناپذیری این مهم معرفی نشده است.

حمله دیگر که کلید-عمومی است، «حملهٔ پیام-محتمل»

- فرض کنید که کلید ۵۶ بیتی ارد با کلید عمومی رمز شد است.
- تحلیل‌گر تمامی کلیدهای ممکن ۵۶ بیتی را با کلید عمومی رمز می‌کند و با تطبیق می‌تواند کلید مخفی رمز شده را کشف کند.

الگوریتم رسا

مقالهٔ هلمن و دیفی

- ایجاد روشی نوآئین در رمزنگاری
- این پیشنهاد چالشی برای رمزنگاران شد
- بسیاری از پیشنهادها مانند کوله‌پشتی دررو مرکل را دچار شکست کرد.

یکی از پاسخ‌های موفق به چالش در ۱۳۵۶

- ران رایوست و ادی شمیر و لن ادلمن در مfم معرفی کردند و در سال بعد به چاپ رساندند.

در شمای رسا

- هم متن اصلی و هم متن رمز اعداد صحیحی بین 0 تا $n - ۱$ برای n خاصی
- اندازه n معمولا ۱۰۲۴ بیت یا ۳۰۹ رقم ده‌دهی است. بنابراین n کوچکتر از $۲^{۱۰۲۴}$

تابع فی اوئلر

$\phi(n)$

- تعداد اعداد طبیعی کوچکتر از **n** و نسبت به **n** اول
- قرارداد: $\phi(۱) = ۱$
- مثال
  - $\phi(۳۷)$
    - چون عدد اول است، پس تمامی اعداد کوچکتر از ۳۷ نسبت اول با آن دارند، در نتیجه $\phi(۳۷) = ۳۶$
  - $\phi(۳۵)$
    - $\phi(۳۵) = ۲۴$

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

قضیهٔ اوئلر

قضیهٔ اوئلر

- برای هر a و n نسبت به هم اول داریم:

$$a^{\phi(n)} \equiv ۱ \pmod{n}$$

شرح شیرین الگوریتم

استفادهٔ رسا از عبارت نمائی

رمز بلوکی متن اصلی

- هر بلوک
  - برابر مقداری کوچکتر از n
- طول بلوک
  - کوچکتر از یا مساوی با $\log_2(n) + 1$
- در عمل اندازه بلوک برابر i
  - به طوری که $2^i < n \leq 2^{i+1}$

رمزگذاری و رمزگشائی برای بلوک متن اصلی M و بلوک متن رمز C دارای اَشکال:

- $C = M^e \% n$
- $M = C^d \% n$
  - $M = C^d \% n = (M^e)^d \% n = C = M^{ed} \% n$

- معلوم بودن مقدار n برای هر دوی فرستنده و گیرنده مقدار n
- فرستنده مقدار e را می‌داند و گیرنده صرفا مقدار d را می‌داند.
- این دستگاه، دستگاه رمز کلید-عمومی با کلید عمومی $\{e,n\}$ و کلید خصوصی $\{d,n\}$

شرح شیرین الگوریتم

شرایط درستی رمزنگاری عمومی

- تعیین e و d و n به نحوی که $M^{ed}\%n = M$ برای تمامی $M < n$
- راحتی نسبی محاسبهٔ $M^{e}\%n$ و $C^{d}\%n$ برای تمامی $M < n$
- نشدنی بودن استنباط d با داشتن e و n

مورد اول

- در صورت خواهانی برقراری رابطهٔ $M^{ed}\%n = M$ زمانی برقرار است که اگر e و d معکوس ضربی به پیمانه $\phi(n)$ باشند و $\phi(n)$ تابع اوئلر است. در مقدمات ریاضی نشان داده شد که برای دو عدد اول p و q داریم $\phi(pq) = (p-۱)(q-۱)$. رابطهٔ بین e و dرا می‌توان به صورت زیر بیان کرد

$$ed\%\phi(n) = ۱$$

که هم ارز با اظهار موارد زیر است:

$$ed \overset{\phi(n)}{\equiv} ۱$$

$$d \overset{\phi(n)}{\equiv} e^{-۱}$$

بنابراین e و d معکوس ضرب به پیمانهٔ $\phi(n)$ هستند. لازم است که طبق قوانین حسب پیمانه‌ای این مورد در صورت صادق است اگر d (در نتیجه e) نسبت به $\phi(n)$ اول باشند. به دیگر سخن، شرط برقراری $(\phi(n),d) = ۱$بم‌م.

شما رسا

جزئیات

p و q دو عدد اول	خصوصی و انتخابی
$n = pq$	عمومی، یافتن از طرییق محاسبه
e با شرط $1 < e < \phi(n)$ و $(\phi(n), d) = 1$ بم‌م	عمومی و انتخابی
$d \equiv e^{-1} \pmod{\phi(n)}$	خصوصی و یافتن از طریق محاسبه

رسا

دستگاه رمز کلید-عمومی با کلید عمومی $\{e,n\}$ و کلید خصوصی $\{d,n\}$

فرضا کاربر الف کلید عمومی خود را منتشر کرده است

کاربر ب به دنبال ارسال پیام M برای الف است.

پس ب $C = M^e \%n$ را حساب می‌کند و C را ارسال می‌کند.

به محض دریافت الف پیام را با حساب $M = C^d \%n$ کشف می‌کند.

رسا

دستگاه رمز کلید-عمومی با کلید عمومی $\{e,n\}$ و کلید خصوصی $\{d,n\}$

فرضا کاربر الف کلید عمومی خود را منتشر کرده است

کاربر ب به دنبال ارسال پیام M برای الف است.

پس ب $C = M^e \% n$ را حساب می‌کند و C را ارسال می‌کند.

به محض دریافت الف پیام را با حساب $M = C^d \% n$ کشف می‌کند. خلاصهٔ رسا:

- تولید کلید
  - انتخاب p و q به نحوی که هر دو اول و $p \neq q$
  - محاسبهٔ $n = p \times q$
  - محاسبهٔ $\phi(n) = (p-1)(q-1)$
  - یافتن عدد صحیح e به طوری‌که $1 < e < \phi(n)$ و $(\phi(n), e)$ب‌م $= 1$
  - محاسبهٔ d از $d \equiv e^{-1} \pmod{\phi(n)}$
  - کلید عمومی $\{e,n\}$ و کلید خصوصی $\{d,n\}$
- رمز با استفاده از کلید عمومی گیرنده
  - متن اصلی: $M < n$
  - متن رمز: $C = M^e \% n$
- کشف رمز با استفاده از کلید خصوصی
  - متن رمز: C
  - متن اصلی: $M = C^d \% n$

رسا

مثال-

۱- انتخاب دو عدد اول $p = ۱۷$ و $q = ۱۱$

۲- حساب $n = pq = ۱۷ \times ۱۱ = ۱۸۷$

۳- حساب $\phi(n) = (p - ۱)(q - ۱) = ۱۶ \times ۱۰ = ۱۶۰$

۴- انتخاب e به طوری که عدد مذکور نسبت به $\phi(n) = ۱۶۰$ اول باشد و از $\phi(n)$ کوچکتر باشد؛ $e = ۷$ را انتخاب می‌کنیم.

۵- dرا طوری انتخاب می‌کنیم که $ed \equiv ۱ \pmod{۱۶۰}$ و $d < ۱۶۰$.

- مقدار درست برابر با $d = ۲۳$ است. چرا که $۱ + (۱۶۰ \times ۱) = ۱۶۱ = ۷ \times ۲۳$. محاسبهٔ dبا تعمیم الگوریتم اقلیدس ممکن است.

رسا

مثال-

بنابراین کلید عمومی $\{۷,۱۸۷\}$ است و کلید خصوصی $\{۲۳,۱۸۷\}$

حال استفاده از کلیدهای مذکور برای $M = ۸۸$

نیاز به محاسبهٔ $C = ۸۸^{۷}\%۱۸۷$:

- $۸۸^{۷}\%۱۸۷ = [(۸۸^{۴}\%۱۸۷) \times (۸۸^{۲}\%۱۸۷) \times (۸۸^{۱}\%۱۸۷)]\%۱۸۷$
- $۸۸^{۱}\%۱۸۷ = ۸۸$
- $۸۸^{۲}\%۱۸۷ = ۷۷۴۴\%۱۸۷ = ۷۷$
- $۸۸^{۴}\%۱۸۷ = ۵۹۹۶۹۵۳۶\%۱۸۷ = ۱۳۲$
- $۸۸^{۷}\%۱۸۷ = (۸۸ \times ۷۷ \times ۱۳۲)\%۱۸۷ = ۸۹۴۴۳۲\%۱۸۷ = ۱۱$

رسا

مثال-

جهت رمزگشائی داریم:

- $۱۱^{۲۳}\%۱۸۷ = [(۱۱^{۸}\%۱۸۷) \times (۱۱^{۸}\%۱۸۷) \times (۱۱^{۴}\%۱۸۷) \times (۱۱^{۲}\%۱۸۷) \times (۱۱^{۱}\%۱۸۷)]\%۱۸۷$
- $۱۱^{۱}\%۱۸۷ = ۱۱$
- $۱۱^{۲}\%۱۸۷ = ۱۲۱$
- $۱۱^{۴}\%۱۸۷ = ۱۴۶۴۱\%۱۸۷ = ۵۵$
- $۱۱^{۸}\%۱۸۷ = ۲۱۴۳۵۸۸۸۱\%۱۸۷ = ۳۳$
- $۱۱^{۲۳}\%۱۸۷ = (۳۳ \times ۳۳ \times ۵۵ \times ۱۲۱ \times ۱۱)\%۱۸۷ = ۷۹۷۲۰۲۴۵\%۱۸۷ = ۸۸$

ریاضی (حساب) پیمانه‌ای

پیمانه

mod

عدد صحیح a و عدد طبیعی n، آنگاه $a \,\%\, n$ برابر است با باقیمانده تقسیم a بر n

یادآوری الگوریتم تقسیم:

$$a = qn + r, \qquad 0 \le r < n; q = \left\lfloor \frac{a}{n} \right\rfloor$$

تغییر نمایش

$$a = \left\lfloor \frac{a}{n} \right\rfloor \times n + a \,\%\, n$$

نمایش صوری عملگر پیمانه

$$a \,\%n = a \; - \left\lfloor \frac{a}{n} \right\rfloor \times n, n \neq 0$$

$$۱۱ \,\%۷ = ۴,$$
$$-۱۱\%۷ = ۳\, n$$

رابطه هم‌نهشتی پیمانه

اظهار اینکه دو ورودی دارای باقیماندهٔ یکسان با توجه به پیمانه داده شده

- مثال (۳ پیمانه)۴ ≡ ۷ یا $۷ \equiv ۴ (mod ۳)$ یا ۴ $\overset{۳}{\equiv}$ ۷
  - هر دوی ۷ و ۴ دارای باقیماندهٔ ۱ به هنگام تقسیم بر ۳
- هم‌ارزی دو رابطهٔ زیر:

$$۷ \equiv ۴ \left(\text{۳ پیمانه}\right) \Leftrightarrow ۷ \% ۳ = ۴ \% ۳$$

- به سخن دیگر، یکسانی $a \equiv b (m$ پیمانه$)$ با مضرب صحیح بودن $a - b$ از m

≡ علامت هم‌نهشتی

استفاده از رابطه هم‌نهشتی در تعریف رده‌های افراز باقی‌مانده‌ها

- اعدادی با باقیمانده یکسان به پیمانه m تشکیل‌دهندهٔ یک رده به پیمانهٔ m
- وجود m رده (کلاس) به پیمانهٔ m

عمل‌های حساب پیمانه‌ای

مجموعه اعداد طبیعی کوچکتر از n

$$Z_n = \{0,۱, \dots, n-۱\}$$

- مشهور به مجموعه باقی‌مانده‌ها به پیمانهٔ n
  - هر عدد نمایش یک رده
  - نمایش با $[0]$ و $[۱]$ و $[۲]$ و ... و $[n-۱]$ به طوری که

$$[r] = \{a: a \in Z, a\}$$

- رده‌های مانده به پیمانهٔ ۴

$$[0] = \{\dots, -۱۶, -۱۲, -۸, -۴, ۰, ۴, ۸, ۱۲, ۱۶, \dots\}$$
$$[۱] = \{\dots, -۱۵, -۱۱, -۷, -۳, ۱, ۵, ۹, ۱۳, ۱۷, \dots\}$$
$$[۲] = \{\dots, -۱۴, -۱۰, -۶, -۲, ۲, ۶, ۱۰, ۱۴, ۱۸, \dots\}$$
$$[۳] = \{\dots, -۱۳, -۹, -۵, -۱, ۳, ۷, ۱۱, ۱۵, ۱۹, \dots\}$$

- انتخاب کوچکترین عدد نامنفی به عنوان نشان رده

رابطه هم‌نهشتی پیمانه

ویژگی‌ها

I. $m|(a-b) \Longrightarrow a \overset{m}{\equiv} b$

II. $a \overset{m}{\equiv} a$

III. $a \overset{m}{\equiv} b \Longrightarrow b \overset{m}{\equiv} a$

IV. $a \overset{m}{\equiv} b, b \overset{m}{\equiv} c \Longrightarrow a \overset{m}{\equiv} c$

V. $a \overset{m}{\equiv} b, c \overset{m}{\equiv} d \Longrightarrow \begin{cases} a + c \overset{m}{\equiv} b + d \\ ac \overset{m}{\equiv} bd \end{cases}$

VI. $a \overset{m}{\equiv} b \Longrightarrow a^k \overset{m}{\equiv} b^k$

موارد II و III و IV به ترتیب نمایش خاصیت‌های بازتابی و تقارن و تراگذری- بنابراین هم‌نهشتی رابطه‌ای هم‌ارزی است.

عمل‌های حساب پیمانه‌ای

عملگر پیمانه m

- نگاشت کنندهٔ تمامی اعداد صحیح به مجموعه‌های $\{0,1,\ldots,(m-1)\}$
- پرسش: امکان تعریف عملیات‌های ریاضی که محدود به مجموعه باقی بمانند.
  - پاسخ مثبت و در روشی به نامه حساب پیمانه‌ای
  - دارای ویژگی‌های

$$[a\ \%\ m + b\ \%\ m]\%\ m = (a+b)\%\ m$$
$$[a\ \%\ m - b\ \%\ m]\%\ m = (a-b)\%\ m$$
$$[a\ \%\ m \times b\ \%\ m]\%\ m = (a\times b)\%\ m$$

- مورد اول $a\ \%\ m = r_a$ و $b\ \%\ m = r_b$
- $\Longleftarrow$ $a = r_a + jm$ و $b = r_b + km$

$$(a+b)\%\ m = (r_a + jm + r_b + km)\%\ m$$
$$= (r_a + r_b)\%\ m$$
$$= [a\ \%\ m + b \text{ پیمانه } m]\%\ m$$

عمل‌های ریاضیات پیمانه‌ای

مثال- ۳ = ۸ % ۱۱ و ۷ = ۸ %۱۵

$$[(۱۱ \% ۸) + (۱۵\% ۸)]\% ۸ = ۱۰\% ۸ = ۲$$
$$(۱۱ + ۱۵)\% ۸ = \% ۸ = ۲$$

$$[(۱۱ \% ۸) - (۱۵\%۸)]\% ۸ = -۴\% ۸ = ۴$$
$$(۱۱ - ۱۵)\% ۸ = -۴\% ۸ = ۴$$

$$[(۱۱ \% ۸) \times (۱۵\% ۸)]\% ۸ = ۲۱\% ۸ = ۵$$
$$(۱۱ \times ۱۵)\% ۸ = ۱۶۵\% ۸ = ۵$$

عمل‌های ریاضیات پیمانه‌ای

مثال-توان‌رسانی

- $۱۱^{۷} \% ۱۳ = ۲$
- با ضرب متوالی

$$۱۱^{۲} = ۱۲۱ \overset{۱۳}{\equiv} ۴$$

$$۱۱^{۴} = (۱۱^{۲})^{۲} \overset{۱۳}{\equiv} ۴^{۲} \overset{۱۳}{\equiv} ۳$$

$$۱۱^{۷} = ۱۱ \times ۱۱^{۲} \times ۱۱^{۴}$$

$$۱۱^{۷} \overset{۱۳}{\equiv} ۱۱ \times ۴ \times ۳ \overset{۱۳}{\equiv} ۲$$

عمل‌های ریاضیات پیمانه‌ای

مثال-

عملیات‌ها به پیمانهٔ ۸

+	۰	۱	۲	۳	۴	۵	۶	۷
۰	۰	۱	۲	۳	۴	۵	۶	۷
۱	۱	۲	۳	۴	۵	۶	۷	۰
۲	۲	۳	۴	۵	۶	۷	۰	۱
۳	۳	۴	۵	۶	۷	۰	۱	۲
۴	۴	۵	۶	۷	۰	۱	۲	۳
۵	۵	۶	۷	۰	۱	۲	۳	۴
۶	۶	۷	۰	۱	۲	۳	۴	۵
۷	۷	۰	۱	۲	۳	۴	۵	۶

جمع به پیمانهٔ ۸

×	۰	۱	۲	۳	۴	۵	۶	۷
۰	۰	۰	۰	۰	۰	۰	۰	۰
۱	۰	۱	۲	۳	۴	۵	۶	۷
۲	۰	۲	۴	۶	۰	۲	۴	۶
۳	۰	۳	۶	۱	۴	۷	۲	۵
۴	۰	۴	۰	۴	۰	۴	۰	۴
۵	۰	۵	۲	۷	۴	۱	۶	۳
۶	۰	۶	۴	۲	۰	۶	۴	۲
۷	۰	7	۶	۵	۴	۳	۲	۱

ضرب به پیمانهٔ ۸

توجه به تفاوت رفتاری جمع و ضرب

w	$-w$	w^{-1}
۰	۰	–
۱	۷	۱
۲	۶	–
۳	۵	۳
۴	۴	–
۵	۳	۵
۶	۲	–
۷	۱	۷

معکوس جمع و ضرب به پیمانهٔ ۸

عمل‌های ریاضیات پیمانه‌ای

مثال-

عملیات‌ها به پیمانهٔ ۷

+	۰	۱	۲	۳	۴	۵	۶
۰	۰	۱	۲	۳	۴	۵	۶
۱	۱	۲	۳	۴	۵	۶	۰
۲	۲	۳	۴	۵	۶	۰	۱
۳	۳	۴	۵	۶	۰	۱	۲
۴	۴	۵	۶	۰	۱	۲	۳
۵	۵	۶	۰	۱	۲	۳	۴
۶	۶	۰	۱	۲	۳	۴	۵

جمع به پیمانهٔ ۷

×	۰	۱	۲	۳	۴	۵	۶
۰	۰	۰	۰	۰	۰	۰	۰
۱	۰	۱	۲	۳	۴	۵	۶
۲	۰	۲	۴	۶	۱	۳	۵
۳	۰	۳	۶	۲	۵	۱	۴
۴	۰	۴	۱	۵	۲	۶	۳
۵	۰	۵	۳	۱	۶	۴	۲
۶	۰	۶	۵	۴	۳	۲	۱

ضرب به پیمانهٔ ۷

w	$-w$	w^{-1}
۰	۰	–
۱	۶	۱
۲	۵	۴
۳	۴	۵
۴	۳	۲
۵	۲	۳
۶	۱	۱

معکوس جمع و ضرب به پیمانهٔ ۷

عمل‌های حساب پیمانه‌ای

- ویژگی‌های حساب پیمانه‌ای اعداد طبیعی در Z_n
  - قوانین جابجاپذیری

$$(w + x)\%n = (x + w)\%n$$
$$(w \times x)\%n = (x \times w)\%n$$

  - قوانین شرکت‌پذیری

$$[(w + x) + y]\%n = [w + (x + y)]\%n$$
$$[(w \times x) \times y]\%n = [w \times (x \times y)]\%n$$

  - قوانین توزیع‌پذیری

$$[w \times (x + y)]\%n = [w \times x + w \times y]\%n$$

  - عضوهای همانی

$$(0 + x)\%n = (x)\%n$$
$$(۱ \times x)\%n = (x)\%n$$

  - معکوس جمع $(-w)$

$$\forall w \in Z_n : \exists z \Longrightarrow w + z \overset{n}{\equiv} 0$$

عمل‌های حساب پیمانه‌ای

قضیه

- اگر a و n دو عدد صحیح نسبت به هم اول هستند
- آن‌گاه، یک عدد منحصر بفرد $x \in Z_n$ داریم که

$$ax\%n = b$$

- مثال در Z_8

$$۳x\%۸ = ۲ \Longrightarrow x = ۶$$

اثبات- تمرین

عمل‌های حساب پیمانه‌ای

ویژگی حساب پیمانه‌ای متفاوت از ریاضی معمول

- همانند جمع معمولی

$$(a+b) \overset{n}{\equiv} (a+c) \Rightarrow b \overset{n}{\equiv} c$$
$$(۵+۲۳) \overset{n}{\equiv} (۵+۷) \Rightarrow ۲۳ \overset{n}{\equiv} ۷$$

- اما ضرب متفاوت! درستی رابطه زیر در صورتی که دو عدد صحیح نسبت به هم اول باشند.

$$\left[\text{ب‌م‌م}(a,n) = ۱, (a \times b) \overset{n}{\equiv} (a \times c)\right] \Rightarrow b \overset{n}{\equiv} c$$

- مثالی جهت درست نبودن ضرب در هر حالتی

$$۶ \times ۳ = ۱۸ \overset{۸}{\equiv} ۲$$
$$۶ \times ۷ = ۴۲ \overset{۸}{\equiv} ۲$$

اما $۳ \overset{۸}{\not\equiv} ۷$

عمل‌های حساب پیمانه‌ای

- اما ضرب متفاوت! درستی رابطه زیر در صورتی که دو عدد صحیح نسبت به هم اول باشند.

$$\left[\text{ب‌م‌م}(a,n) = ۱, (a \times b) \overset{n}{\equiv} (a \times c)\right] \Longrightarrow b \overset{n}{\equiv} c$$

دلیل

- هر پیمانهٔ n و ضریب a جهت تولید اعداد 0 تا $n - ۱$
  - شکست در تولید مجموعهٔ تمام مانده‌ها اگر a و n دارای شمارندهٔ مشترک باشند.

عمل‌های حساب پیمانه‌ای

- $a = ۶$ و $n = ۸$

$Z_۸$	۷	۶	۵	۴	۳	۲	۱	0
ضرب در ۶	۴۲	۳۶	۳۰	۲۴	۱۸	۱۲	۶	0
مانده‌ها	۲	۴	۶	0	۲	۴	۶	0

- $a = ۵$ و $n = ۸$

$Z_۸$	۷	۶	۵	۴	۳	۲	۱	0
ضرب در ۶	۳۵	۳۰	۲۵	۲۰	۱۵	۱۰	۵	0
مانده‌ها	۳	۶	۱	۴	۷	۲	۵	0

- عدد صحیحی دارای «معکوس ضربی» در Z_n است اگر و فقط اگر عدد مذکور نسبت به **n** اول باشد.

قضیهٔ فرما

قضیهٔ فرما

- p عدد اول و a عدد طبیعی با شرط $p \nmid a$، آن‌گاه

$$a^{p-1} \overset{p}{\equiv} 1$$

- اثبات
- $A = \{0,1,2, \dots, p-1\}$ مجموعه کامل مانده‌ها به پیمانهٔ p
- $p \nmid a \Longrightarrow$ ب‌م‌م$(a,p) = 1$
- $B = \{0,a,2a, \dots, (p-1)a\}$ به طریق اولی دستهای کامل مانده‌ها به پیمانهٔ p
- با کنار گذاشتن صفر از هر دو مجموعه داریم:

$$a \times 2a \times \cdots \times (p-1)a \overset{p}{\equiv} 1 \times 2 \times \cdots \times p-1$$

$$\Longrightarrow a^{p-1}(1 \times 2 \times \cdots \times p-1) \overset{p}{\equiv} 1 \times 2 \times \cdots \times p-1$$

$$\Longrightarrow a^{p-1}(p-1)! \overset{p}{\equiv} (p-1)!$$

- $(p-1)!$ نسبت به p اول،پس

$$a^{p-1} \overset{p}{\equiv} 1$$

- حکم ثابت است.

قضیهٔ فرما

قضیهٔ فرما

- p عدد اول و a عدد طبیعی با شرط $p \nmid a$، آن‌گاه

$$a^{p-1} \overset{p}{\equiv} 1$$

قضیهٔ چینی باقیمانده

p و q دو عدد صحیح نسبت به هم اول

اگر $a\%p = x$ و $a\%q = x$

- آن‌گاه $a\%pq = x$

- مثال $۳۷\%۵ = ۲$ و $۳۷\%۷ = ۲$، پس $۳۷\%۳۵ = ۲$

اثبات

- فرض $b\%pq = x$ و $b < pq$، کافی است نشان دهیم $b = a$
- داریم $a\%p = x \Longleftarrow \left.\begin{matrix} a\%p = b \\ a\%q = b \end{matrix}\right\} \Longleftarrow b = pt_۱ + a = qt_۲ + a$
- $pt_۱ = qt_۲ \Longleftarrow$ مضرب مشترک p و q
  - اما کم‌م برابر با pq و چون $b < pq$
    - درنتیجه $pt_۱ = qt_۲ = 0$

رسا- اثبات درستی

- تولید کلید
  - انتخاب p و q به نحوی که هر دو اول و $p \neq q$
  - محاسبهٔ $n = p \times q$
  - محاسبهٔ $\phi(n) = (p - ۱)(q - ۱)$
  - یافتن عدد صحیح e به طوری‌که $۱ < e < \phi(n)$ و $(\phi(n), e)$ب‌مم $= ۱$
  - محاسبهٔ d از $d \equiv e^{-۱} \pmod{\phi(n)}$
  - کلید عمومی $\{e, n\}$ و کلید خصوصی $\{d, n\}$

رسا- اثبات یکتایی کلید

- تولید کلید
  - انتخاب p و q به نحوی که هر دو اول و $p \neq q$
  - محاسبهٔ $n = p \times q$
  - محاسبهٔ $\phi(n) = (p - ۱)(q - ۱)$
  - یافتن عدد صحیح e به طوری‌که $۱ < e < \phi(n)$ و $(\phi(n), e)$ب‌مم $= ۱$
  - محاسبهٔ d از $d \equiv e^{-۱} \pmod{\phi(n)}$
  - کلید عمومی $\{e,n\}$ و کلید خصوصی $\{d,n\}$

رسا- اثبات یکتایی کلید

محاسبهٔ d از e^{-1} $\overset{\phi(n)}{\equiv}$ d

اثبات منحصر بفردی d:

- قضیه
  - اگر a و n دو عدد صحیح نسبت به هم اول هستند
  - آن‌گاه، یک عدد منحصر بفرد $x \in Z_n$ داریم که

$$ax\%n = b$$

اثبات اول بودن d نسبت به $\phi(n)$:

- t بم‌م d و $\phi(n)$
  - $d = c_1 t$ و $\phi(n) = c_2 t$
- از $ed\%\phi(n) = 1$ داریم: $ed = c_3\phi(n) + 1$

$$ec_1 t = c_3 c_2 t + 1 \Longrightarrow t(ec_1 - c_3 c_2) = 1 \Longrightarrow t = 1$$

تابع فی اوئلر

$\phi(n)$

- تعداد اعداد طبیعی کوچکتر از **n** و نسبت به **n** اول
- قرارداد: $\phi(۱) = ۱$
- مثال
  - $\phi(۳۷)$
    - چون عدد اول است، پس تمامی اعداد کوچکتر از ۳۷ نسبت اول با آن دارند، در نتیجه $\phi(۳۷) = ۳۶$
  - $\phi(۳۵)$
    - $\phi(۳۵) = ۲۴$

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

تابع فی اوئلر

- اگر p عدد اول، آن‌گاه $\phi(p) = p - ۱$
- اگر p و q اعداد اول باشند و $p \neq q$. n=pq، آن‌گاه
$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p - ۱)(q - ۱)$$
- اگر p عدد اول، آن‌گاه $\phi(p^k) = p^k - p^{k-۱}$
- اگر m و n نسبت به هم اول باشند، آن‌گاه $\phi(mn) = \phi(m)\phi(n)$
- اگر $a > ۱$ به صورت $a = p_۱^{a_۱} \times p_۲^{a_۲} \times \cdots \times p_t^{a_t}$ باشد،آن‌گاه
$$\phi(a) = a\left(۱ - \frac{۱}{p_۱}\right)\left(۱ - \frac{۱}{p_۲}\right)\ldots\left(۱ - \frac{۱}{p_t}\right)$$

قضیهٔ اوئلر

قضیهٔ اوئلر

- برای هر a و n نسبت به هم اول داریم: $a^{\phi(n)} \overset{n}{\equiv} ۱$

اثبات–حالت دوم اثبات ادعا برای هر مقدار صحیح از n

- $\phi(n)$ تعداد اعداد «طبیعی» کوچکتر از n و اول نسبت به آن
  - فرض اعداد مورد نظر شامل $R = \{x_۱, x_۲, \dots, x_{\phi(n)}\}$ با شرط هر $x_i \in R$ عدد صحیح متمایز و یکهٔ کوچکتر از n با $(x_i, n) = ۱$ بم‌م
- ضرب مقدار a در هر عضو مجموعهٔ مذکور به پیمانهٔ n:
  - $S = \{(ax_۱ \text{ پیمانه } n), (ax_۲ \text{ پیمانه } n), \dots, (ax_{\phi(n)} \text{ پیمانه } n)\}$
  - ادعا S جایگشتی از R
    - چون a نسبت به n اول و x_i نسبت به n اول $\Leftarrow ax_i$ نیز نسبت به n اول $\Leftarrow$ تمامی اعضای S عدد صحیح کوچکتر از n و نسبت به آن اول
    - عدم وجود تکرار در S
      - یادآوری $(a \times b) \overset{n}{\equiv} (a \times c) \Rightarrow b \overset{n}{\equiv} c$ بم‌م $(a, n) = ۱$
      - $(a \times x_i) \overset{n}{\equiv} (a \times x_j) \Rightarrow x_i \overset{n}{\equiv} x_j$ و در این حالت یعنی $x_i = x_j$ که تناقض است

قضیهٔ اویلر

اثبات-حالت دوم اثبات ادعا برای هر مقدار صحیح از n

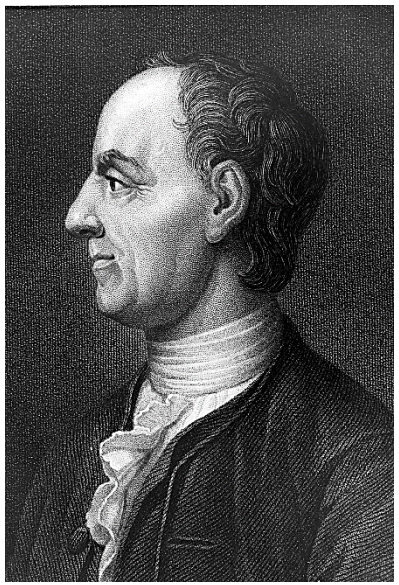
- $\phi(n)$ تعداد اعداد «طبیعی» کوچکتر از n و اول نسبت به آن
  - فرض اعداد مورد نظر شامل $R = \{x_1, x_2, \dots, x_{\phi(n)}\}$ با شرط هر $x_i \in R$ عدد صحیح متمایز و یکهٔ کوچکتر از n با $(x_i, n) = 1$ بم‌م
- ضرب مقدار a در هر عضو مجموعهٔ مذکور به پیمانهٔ n:
  - $S = \{(ax_1 \text{ پیمانه } n), (ax_2 \text{ پیمانه } n), \dots, (ax_{\phi(n)} \text{ پیمانه } n)\}$
  - ادعا S جایگشتی از R
    - چون a نسبت به n اول و x_i نسبت به n اول $\Leftarrow ax_i$ نیز نسبت به n اول $\Leftarrow$ تمامی اعضای S عدد صحیح کوچکتر از n و نسبت به آن اول
    - عدم وجود تکرار در S
      - یادآوری $(a, n) = 1, (a \times b) \overset{n}{\equiv} (a \times c) \Rightarrow b \overset{n}{\equiv} c$ بم‌م
      - $(a \times x_i) \overset{n}{\equiv} (a \times x_j) \Rightarrow x_i \overset{n}{\equiv} x_j$ و در این حالت یعنی $x_i = x_j$ که تناقض است
- در ادامه

$$\prod_{i=1}^{\phi(n)} (ax_i \,\%n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)} ax_i \overset{n}{\equiv} \prod_{i=1}^{\phi(n)} x_i$$

$$a^{\phi(n)} \left[\prod_{i=1}^{\phi(n)} x_i \right] \overset{n}{\equiv} \prod_{i=1}^{\phi(n)} x_i$$

$$a^{\phi(n)} \overset{n}{\equiv} 1$$



https://kids.britannica.com/students/article/Leonhard-Euler/274225

قضیهٔ اوئلر

قضیهٔ اوئلر

- برای هر a و n نسبت به هم اول داریم: $a^{\phi(n)} \overset{n}{\equiv} 1$

$$a = 3; n = 10; \phi(10) = 4; \quad a^{\phi(n)} = 3^4 = 81 = 1(\text{mod } 10) = 1(\text{mod } n)$$
$$a = 2; n = 11; \phi(11) = 10; \quad a^{\phi(n)} = 2^{10} = 1024 = 1(\text{mod } 11) = 1(\text{mod } n)$$

قضیهٔ اوئلر

اوئلر اثبات‌کنندهٔ قضیهٔ فرما و سپس تعمیم آن

قضیهٔ اوئلر

- برای هر a و n نسبت به هم اول داریم:

$$a^{\phi(n)} \overset{n}{\equiv} ۱$$

- نتیجه-برای هر a و n نسبت به هم اول داریم:

$$a^{\phi(n)+۱} \overset{n}{\equiv} a$$

رسا- اثبات درستی رمز و کشف

- رمز با استفاده از کلید عمومی گیرنده
  - متن اصلی: $M < n$
  - متن رمز: $C = M^e \% n$
- کشف رمز با استفاده از کلید خصوصی
  - متن رمز: C
  - متن اصلی: $M = C^d \% n$

رسا- اثبات درستی رمز و کشف

فرض‌ها

- $(p,q) = ۱$ ب‌م‌م
- $n = pq$
- $ed\%\phi(n) = ۱$

حکم

- $\forall M \in Z_n : (M^e)^d \% n = \mathrm{M}$

- اثبات: با داشتن $M \in Z_n$ دو مورد ممکن جهت تحلیل
  - الف) $(M,n) = ۱$ ب‌م‌م
  - ب) $(M,n) \neq ۱$ ب‌م‌م

رسا- اثبات درستی رمز و کشف

مورد اول $(M,n) = ۱$ بم‌م

- صحت قضیهٔ اوئلر و امکان استفاده از آن

$$M^{\phi(n)} \overset{n}{\equiv} ۱$$

- بر اساس فرض $ed\%\phi(n) = ۱$

$$(M^e)^d = M^{ed} = M^{۱+k\phi(n)}$$
$$M^{۱+k\phi(n)} = M.M^{k\phi(n)} = M.\left(M^{\phi(n)}\right)^k$$

قضیه اوئلر

$$M.\left(M^{\phi(n)}\right)^k \% n = M$$

رسا- اثبات درستی رمز و کشف

مورد دوم $(M,n) \neq$ ۱ بم‌م

عدم صحت قضیهٔ اوئلر و متعاقبا عدم‌امکان استفاده از آن

استفاده از ق‌چ‌ب

- p و q دو عدد صحیح نسبت به هم اول و اگر $a\%p = x$ و $a\%q = x$، آن‌گاه $a\%pq = x$
- بنابراین نیاز به اثبات دو گزارهٔ $(M^e)^d\%p = M$ و $(M^e)^d\%q = M$ جهت رسیدن به نتیجه مطلوب
- جهت اثبات: چون $(M,n) \neq$ ۱ بم‌م
  - یا $(M,n) = p$ بم‌م یا $(M,n) = q$ بم‌م
  - بدون از دست رفتن عمومیت فرض بر $(M,n) = p$ بم‌م
    - چگونه عمومیت باقی می‌ماند؟
  - $m = kp$ و $m\%p = 0$

$$(M^e)^d = \left((kp)^e\right)^d$$

- بنابراین، بخش اول منجر به ضریبی از p در نتیجه برابر صفر. گزاره اول اثبات و برآورده‌کنندهٔ $0 = 0$

رسا- اثبات درستی رمز و کشف

- گزارهٔ دوم
- داریم $(M,n) = ۱$ ب‌م‌م، براورده کردن شروط قضیهٔ اوئلر $M^{\phi(q)}\%q = ۱$
- منجر به

$$(M^e)^d = M^{ed} = M^{ed-۱}M$$
$$= M^{h(p-۱)\,(q-۱)}.M = \left(M^{(q-۱)}\right)^{h(p-۱)}.M = (۱)^{h(p-۱)}.M = M\%q$$

- اثبات گزارهٔ دوم
- حکم برقرار است.

یافتن معکوس جمع پیمانه‌ای

یافتن معکوس عدد a به پیمانهٔ m

همیشه موجود

بررسی تمامی $a + km$ –و یافتن موردی که در بازهٔ $\{0,1, \dots, m-1\}$ قرار می‌گیرد

یافتن معکوس ضرب پیمانه‌ای

سه روش

- جستجوی کامل
- استفاده از الگوریتم گسترش اقلیدس

$$ax + my = 1 \Rightarrow ax + my \overset{m}{\equiv} ۱ \Rightarrow ax \overset{m}{\equiv} ۱ \Rightarrow x$$

- استفاده از قضیهٔ فرما (قضیهٔ کوچک فرما)

$$a^{m-۱} \overset{m}{\equiv} ۱ \Rightarrow aa^{m-۲} \overset{m}{\equiv} ۱ \Rightarrow a^{m-۲} \Rightarrow a^{m-۲}\%\mathrm{m}$$

مثال

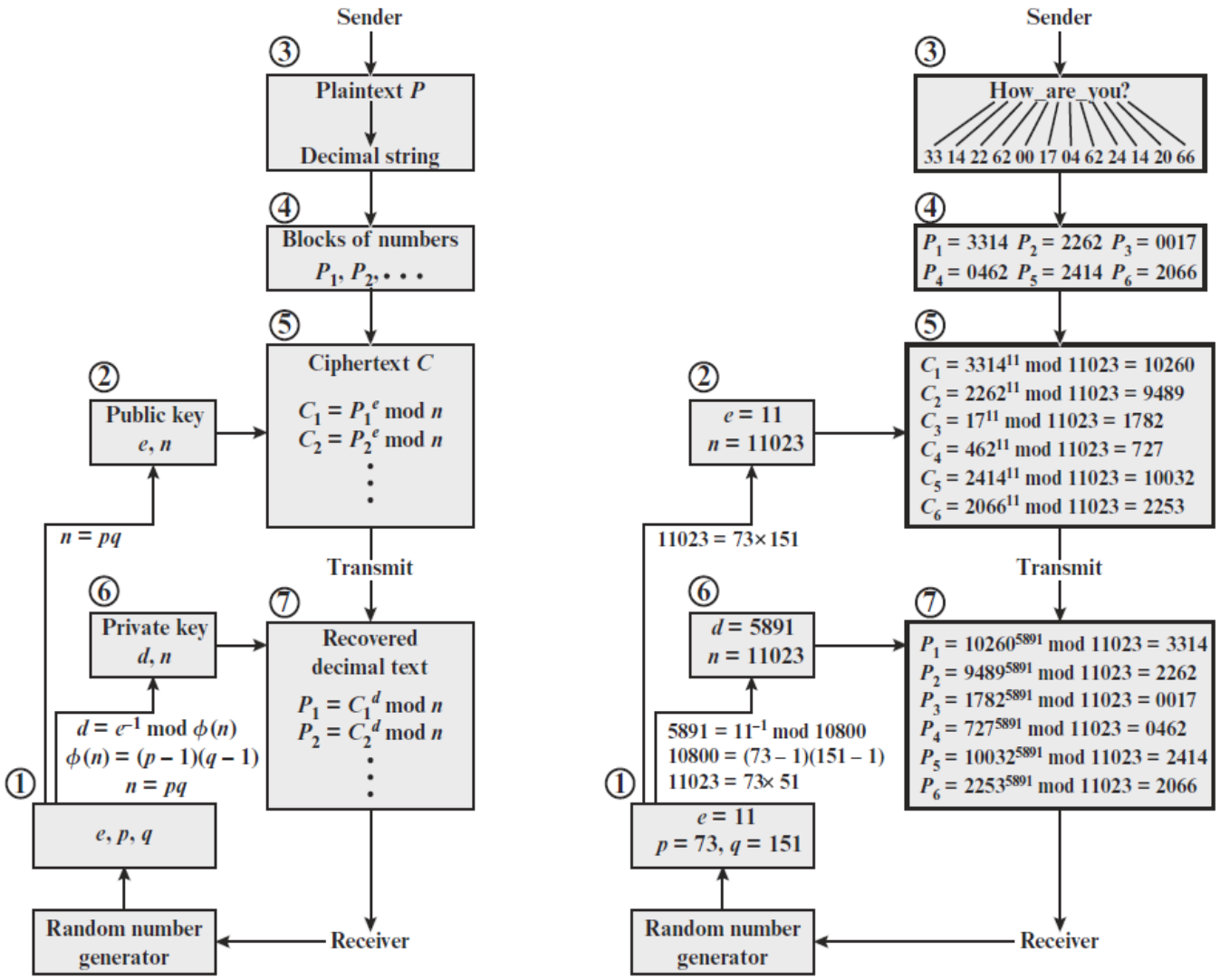


Figure 9.7 RSA Processing of Multiple Blocks

جنبه‌های رایانشی

دو مسئله از لحاظ پیچیدگی وجود دارد. یکی فرایند رمزگذاری/گشائی و دیگری تولید کلید.

حساب پیمانه‌ای نمائی- هر دو بخش رمز و کشف درگیر به توان رسیدن عددی با استفاده از عددی دیگر هستند که سپس بااقیمانده به پیمانه n به دست می‌آید. همان‌طور که مثال‌ها نشان دادند می‌توان از خواص حساب پیمانه‌ای استفاده برد:

$$[(a\%n) \times (b\%n)]\%n = (a \times b)\%n$$

بنابراین می‌توان نتایج میانی را کاهش داد. و در واقع انجم محاسبات را عملی می‌کند.

مورد دیگر کارائی توان رسانی است. در رسا با نماهای محتملا بزرگ سروکار داریم. روش مستقیم تک تک ضرب‌ها انجام می‌پذیرد. اما همان‌طور که در مثال ها یمشخص است می‌توان از که تکه کردن بهره برد. همچنین

تولید کلید

پیش از عملیات کلید عمومی نیاز است تا جفتی از کلیدها تولید شود. اینکار شامل فعالیت‌های زیر است

انتخاب دو عدد اول pو q

انتخاب e یا d و حساب دیگری

جهت جلوگیری از امکان محاسبه n نیاز است که pو q بزرگ باشند. از طرف دیگر روش یافتن عدد اول بزرگ باید تا حد معقولی کارا باشد.

در حال حاضر روش مناسبی برای دستیابی به ادعداد اول بزرگ وجود ندارد. بنابراین روش‌های دیگری برای حل مسئیله باید یافت. رویه اینگونه است که عدد فرد بزرگی را تصادفی تولید کرد و بررسی کرد که اول هست یا نه. در صورت رد عدد، عدد تصادفی دیگری امتحان می‌شود تا آزمون اولی را بگذراند. روش‌های زیادی وجود دارد× تقریبا تمامی آزمون‌ها احتمالی هستند. میلر-رابین از این دست است. البته روش مذکور هنگامی که نیاز به کلید جدید باشد استفاده می‌شود. نیاز به امتحان LN(N) عدد است. استفاده از تعمیم اقلیدس برای یافتن d یا e.

احتمال نسبت به هم اول بودن دو عدد برابر ۰,۶ است پس محاسبات آنچنانی نمی‌خواهد .

امنیت رسا

جستجو کامل- امتحان تمامی کلیدها

- راه‌حل- فضای کلید بزرگ، تعداد بیشتر بیت‌های d
- همزمان توجه به عدم افزایش زیاد زمان رمزگذاری/رمزگشائی

حملات ریاضی- تجزیهٔ ضرب دو عدد اول

- سه نوع روش متفاوت داریم
  - تجزیهٔ n به دو عدد اول که بر اساس آن $\phi(n)$ و محاسبهٔ $e^{-1} \overset{\phi(n)}{\equiv} d$ می‌شود
  - مستقیما یافتن $\phi(n)$ و محاسبهٔ $e^{-1} \overset{\phi(n)}{\equiv} d$ می‌شود.
  - مستقیما یافتن d

منابع

[هلمن و دیفی]

[شمیر و دیگران]

[استالینگز]

[لاودن]

- https://appsrv.cse.cuhk.edu.hk/~taoyf/course/bmeg3120/fall13/www/
- https://crypto.stackexchange.com/questions/2884/rsa-proof-of-correctness