امنیت داده ها

فصل نهم : رمزنگاری کلید عمومی «الجمل» و مبادله کلید «دیفی-هلمن»

دکتر یعقوب فرجامی

عضو هیات علمی دانشکده فنی قم

Z2

- $Z2=\{0,1\}$, و $Z2^*=\{1\}$
- $<1>^+$
- $<1>^+ =\{1,0\}=Z2$, 1 مولد جمعی است
- $<1>^* =\{1\}=Z2^*$, 1 مولد ضربی است

Z3

- $Z3=\{0,1,2\}$, و $Z3^*=\{1,2\}$
- $<1>^+ =\{1,2,0\}=Z3$, 1 مولد جمعی است
- $<1>^* =\{1\}\#Z3^*$, 1 مولد ضربی نیست
- $<2>^+ =\{2,1,0\}=Z3$, 2 مولد جمعی است
- $<2>^* =\{2,1\}=Z3^*$, 2 مولد ضربی است

Z4

- $Z4=\{0,1,2,3\}$, و $Z4^*=\{1,2,3\}$
- $<1>^+ =\{1,2,3,0\}=Z4$, 1 مولد جمعی است
- $<1>^* =\{1\}\#Z4^*$, 1 مولد ضربی نیست
- $<2>^+ =\{2,0\}\#Z4$, 2 مولد جمعی نیست
- $<2>^* =\{2,0\}\#Z4^*$, 2 مولد ضربی نیست
- $<3>^+ =\{3,2,1,0\}=Z4$, 3 مولد جمعی است
- $<3>^* =\{3,1\}\#Z4^*$, 3 مولد ضربی نیست

Z5

- $Z5=\{0,1,2,3,4\}$, و $Z5^*=\{1,2,3,4\}$
- 2 مولد جمعی است, $<2>^{+}=\{2,4,1,3,0\}=Z5$
- 2 مولد ضربی است, $<2>^{*}=\{2,4,3,1\}=Z5^*$
- 3 مولد جمعی است, $<3>^{+}=\{3,1,4,2,0\}=Z5$
- 3 مولد ضربی است, $<3>^{*}=\{3,4,2,1\}=Z5^*$
- 4 مولد جمعی است $<4>^{+}=\{4,3,2,1,0\}$
- 4 مولد ضربی نیست, $<4>^{*}=\{4,1\}\#Z5^*$

Z6

- $Z6=\{0,1,2,3,4,5\}$, و $Z6^*=\{1,2,3,4,5\}$
- $<2>^{+}=\{2,4,0\}\#Z6$, 2 مولد جمعی نیست
- $<2>^{*}=\{2,4\}\#Z6^*$, 2 مولد ضربی نیست
- $<3>^{+}=\{3,0\}\#Z6$, 3 مولد جمعی نیست
- $<3>^{*}=\{3\}\#Z6^*$, 3 مولد ضربی نیست
- مشابها خواهیم دید 4 و 5 هم مولد ضربی و جمعی نیستند

Z7

- $Z7=\{0,1,2,3,4,5,6\}$, و $Z7^*=\{1,2,3,4,5,6\}$
- $\langle 2\rangle^+ =\{2,4,6,1,3,5,0\}=Z7$, 2 مولد جمعی است
- $\langle 2\rangle^* =\{2,4,1\}\#Z7^*$, 2 مولد ضربی نیست
- $\langle 3\rangle^+ =\{3,6,2,5,1,4,0\}=Z7$, 3 مولد جمعی است
- $\langle 3\rangle^* =\{3,2,6,4,5,1\}=Z7^*$, 3 مولد ضربی است
- $\langle 4\rangle^+ =\{4,1,5,2,6,3,0\}=Z7$ 4 مولد جمعی است
- $\langle 4\rangle^* =\{4, 2, 1\}\#Z7^*$, 4 مولد ضربی نیست
- $\langle 5\rangle^+ =\{5,3,1,6,4,2,0\}=Z7$, 5 مولد جمعی است
- $\langle 5\rangle^* =\{5,4,6,2,3,1\}=Z7^*$, 5 مولد ضربی است
- 6 هم بدلیل برابر بودن با 1- نمیتواند مولد ضربی باشد

Z7

- $Z7^*=\{1,2,3,4,5,6\}$ و $Z7=\{0,1,2,3,4,5,6\}$,
- 5 مولد جمعی است $<5>^+ =\{5,3,1,6,4,2,0\}=\{5k, k=1,2, \ldots\}=Z7$,

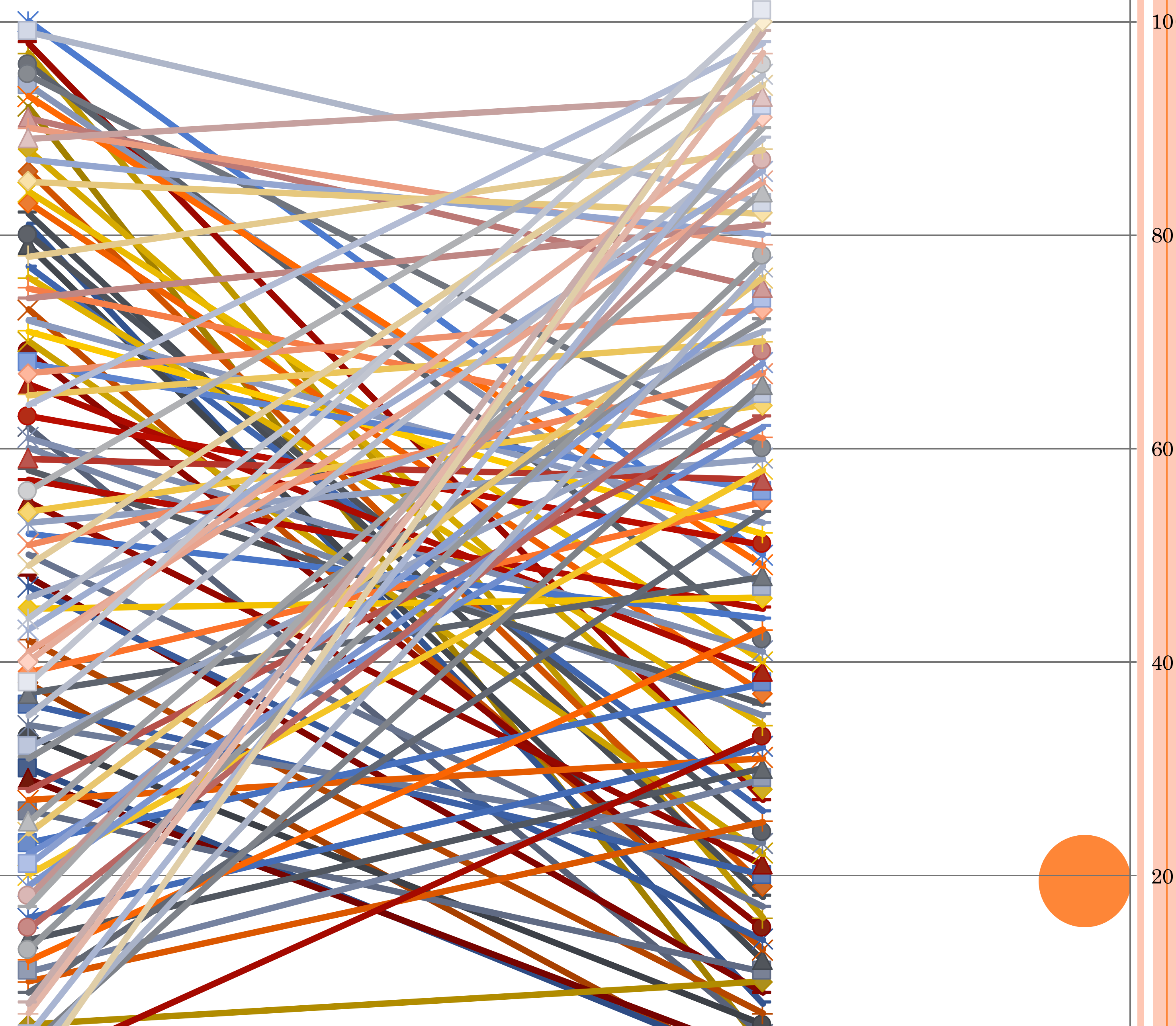
- 5 مولد ضربی است $<5>^* =\{5,4,6,2,3,1\}=\{5^k, k=1,2,\ldots\}=Z7^*$,
- در اینجا داریم $DLOG(4;Z7;5)=2$ یعنی $5^2=4$
- مشابها $DLOG(6;Z7;5)=3$ یعنی $5^3=6$
- همچنین $DLOG(1;Z7;5)=6$ یعنی $5^6=1$
- نگاشت $DLOG(x;Zn;a)$ < -----x یعنی نگاشت لگاریتم گسسته در

Zn نگاشتی قویا در هم ریز است!!!

همینطور است نگاشت a^x < -----x به تصاویر زیر نگاه کنید،

ZN

- N=101,
- A=25



- بر اساس موارد ذکر شده قبلی با داشتن x, a پیدا کردن b به قسمیکه
- $a^b=x$ یعنی $b=DLOG(x;Zn;a)$ کاری دشوار است. که اساسا مبتنی بر محاسبه همه مراحل میباشد.
- روش مستقیم و سر راست محاسبه DLOG به صورت تکرار تا رسیدن به هدف $O(n)$ میباشد،
- اگر $n=2^k$ آنگاه $O(k*2^k)$ خواهد بود. بعبارت دیگر برحسب تعداد ارقام n الگوریتمی نمایی است (دشوار)
- البته با اصلاحات و بهبودهای محاسباتی امکان محاسبه DLOG با پیچیدگی کمتر وجود دارد که بعدا خواهیم گفت.
- نتیجه اخلاقی اینکه DLOG دشواری نمایی دارد.
- همین مسئله مارا کمک میکند که یک پایه تئوری برای رمزنگاری داشته باشیم،
- r کلید خصوصی و $s=a^r \bmod n$ کلید عمومی

Digital Signature with DSS

- الگوریتمی برای امضاء دیجیتال طبق Digital Signature Standard(DSS)
- چکیده پیام با SHA-1
- رمزنگاری چکیده با روش طاهرالجمل
- ***پارامترهای لازم:***
  - عدد اول q به طول ۱۶۰ بیت $2^{159} < q < 2^{160}$
  - انتخاب عدد اول p به طول L بیت $512 < L < 1024$
  - $q \mid p-1$ یا $p = mq + 1$
  - انتخاب عدد تصادفی h بطوریکه

$h \le p-1$, $g = h^{(p-1)/q} \bmod p = h^m$, $g \ge 1$

توجه کنید که g^q=(h^((p-1)/q))*q)=h^(p-1)=h^(phi(p))=1

پس حتما g مولد نیست،

Digital Signature with DSS

- ***پارامترهای لازم (ادامه) :***
  - انتخاب عدد تصادفی بزرگ x ، $0 < x < q$ (x را میخواهیم بعنوان کلید خصوصی استفاده نماییم)
  - محاسبه y ، $y = g^x \bmod p$
  - انتخاب عدد تصادفی k ، $0 < k < q$
- *پارامترهای عمومی* $(p,\ q,\ g,\ \underline{y})$
- *پارامترهای خصوصی* $(k,\ \underline{x,\ h})$

Digital Signature with DSS

- ***الگوریتم امضاء***
- بعد از آماده کردن پارامترها، کاربر می خواهد پیام M خود را امضاء نماید
- به ازای هر پیام جدید می توان k متفاوتی انتخاب کرد
- محاسبه عدد r، $r = (g^k \bmod p) \bmod q$
- محاسبه چکیده پیام، $m = SHA\text{-}1(M)$
- محاسبه عدد s، $s = (k^{-1} .(m + x.r)) \bmod q$
  - نکته : k^{-1} معکوس ضربی عدد k به پیمانه q است

$k.k^{-1} \bmod q = 1$

- اعداد *__r__* و *__s__* امضای دیجیتال پیام M هستند (طول امضاء در DSS حداکثر ۳۲۰ بیت خواهد بود)

Digital Signature with DSS

- ***الگوریتم اعتبار سنجی امضاء***
- محاسبه معکوس s به پیمانه q، $w = s^{-1} \bmod q$
- محاسبه مجدد چکیده پیام، $m = \text{SHA-1}(M)$
- محاسبه عدد u_1، $u_1 = m.w \bmod q$
- محاسبه عدد u_2، $u_2 = r.w \bmod q$
- محاسبه عدد v، $v = ((g^{u1}.y^{u2}) \bmod p) \bmod q$
- اگر v با r (یکی از پارامترهای دریافتی) برابر بود، امضاء <u>معتبر</u> است

Digital Signature with DSS

- ***اثبات درستی الگوریتم DSS***
- با فرض درستی دو لم زیر

$g^q \equiv 1 \pmod p$

$m \equiv n \pmod q \rightarrow g^m \equiv g^n \pmod p$

1. $w = (s)^{-1} \bmod q$
2. $u_1 = \text{SHA-1}(M).w \bmod q$
3. $u_2 = r.w \bmod q$
4. $v = ((g^{u1}.y^{u2}) \bmod p) \bmod q$

$= ((g^{\text{SHA-1}(M).w}.y^{r.w}) \bmod p) \bmod q$

$= ((g^{\text{SHA-1}(M).w}.g^{x.r.w}) \bmod p) \bmod q$

$= ((g^{(\text{SHA-1}(M)+x.r).w}) \bmod p) \bmod q$

Digital Signature with DSS

- ***اثبات درستی الگوریتم DSS ...***

1. $s = (k^{-1}.(\text{SHA-1}(M) + x.r)) \bmod q$
2. $\rightarrow\ w = (k.(\text{SHA-1}(M) + x.r)^{-1}) \bmod q$
3. $(\text{SHA-1}(M) + x.r).w \bmod q = k \bmod q$

- با استناد به لم یک

$$v = (g^k \bmod p) \bmod q = r$$

El Gamal Key Generation

- آلیس عدد اول بزرگ p را انتخاب می کند
- از مجموعه Z_p مولدی به نام g را برمی گزینند (یک مولد به عددی گفته می شود که کوچکتراز p و نسبت به آن اول باشد، و اگر به توان های 0 تا $p-2$ برسد، همه اعداد 1 تا $p-1$ را تولید کند)
- آلیس عدد $\boldsymbol{\alpha}$ را به عنوان <u>*کلید خصوصی*</u> خود با شرط زیر انتخاب می کند

$$1 \leq \alpha \leq p-2$$

- آلیس عدد $\boldsymbol{\beta}$ را به عنوان <u>*کلید عمومی*</u> خود به صورت زیر محاسبه می کند

$$\beta = g^{\alpha} \mod p$$

El Gamal Encryption (Public Key)

- باب میخواهد متن خود را برای آلیس رمز کند به نحویکه فقط آلیس با استفاده از کلید خصوصی خود بتواند آن را رمزگشایی نماید؛
- باب متن خود را به بلوک هایی تقسیم می کند ...... $m1, m2, m3,$
- به قسمیکه $0 \le m_i \le p\text{-}1$
- باب یک عدد کاملاً تصادفی بنام k انتخاب می کند $1 \le k \le p\text{-}2$
- هر بلوک m را به صورت زیر برای آلیس می فرستد

$$m \rightarrow (\gamma , \delta)=(g^k \bmod p , m . \beta^k \bmod p)$$
$$=(g^k \bmod p , m . (g^\alpha)^k \bmod p)$$
$$=(g^k \bmod p , m . (g^k)^\alpha \bmod p)$$

$$\gamma = g^k \bmod p$$
$$\delta = m . \beta^k \bmod p$$

نکته : k برای هر بلوک می تواند تغییر کند

El Gamal Decryption (Private Key)

- آلیس (دارنده کلید خصوصی) به صورت زیر شروع به رمزگشایی می کند

$(\gamma^{p-1} /(\gamma^{\alpha})) * \delta \bmod p = (\gamma^{p-1-\alpha}) * \delta \bmod p$

$= ((g^k)^{p-1} /(g^{k\alpha})) . m . (g^{\alpha})^k \bmod p$

$= m . (g^k)^{p-1} \bmod p$

$= m . 1 \bmod p$

$= m$

پیچیدگی لگاریتم گسسته برای الگوریتم الجمل

- x و y اعدادی صحیح و g یک ریشه اولیه برای میدان Z_p است و داریم :

$$y \equiv g^x \bmod p$$

- عدد y که مخالف صفر است $(1 \le y \le p\text{-}2)$ با یکی از توان های g هم نهشت است و داریم :

$$x \equiv (DLOG_g\, y) \bmod p$$

لگاریتم گسسته

- <u>نکات</u>

همانند لگاریتم پیوسته داریم :

$$DLOG_g\, g = 1 ,\; DLOG_g\, 1 = 0$$

$$g^{DLOG_{g,p}\, a} \bmod p = a$$

پیچیدگی لگاریتم گسسته برای الگوریتم الجمل ...

- نتیجه ۱ :

$$DLOG_{g,\,p}\,(x \times y) = [DLOG_{g,\,p}\,x + DLOG_{g,\,p}\,y] \bmod (p-1)$$

- نتیجه ۲ :

$$DLOG_{g,\,p}\,x^{r} = [r \times DLOG_{g,\,p}\,(x)] \bmod (p-1)$$

- پیچیدگی زمانی حل لگاریتم گسسته :

$$e^{\sqrt[3]{Ln\,p}\,\times\,\sqrt[3]{(Ln(Ln\,p))^2}}$$

- فقط مقدار p تعیین کننده حجم محاسبات است
- سرقت کردن و کشف کردن کلید خصوصی (α) از روی کلید عمومی با این روش بسیار مشکل است

$\beta = g^{\alpha} \bmod p$ (کلید عمومی)

$\alpha = DLOG_{g,\,p}\,(\beta)$

الگوریتم مبادله دیفی هلمن

- یکی از بزرگترین معضلات سیستم های رمزنگاری ، چگونگی تحویل یا دریافت کلید از طرف مقابل است.
- دربرخی از محیط ها مسئله به سادگی حل و فصل می شود(تحویل مستقیم و دستی) !
- به عنوان مثال در سیستم های بانکی یااعتباری ، شخص متقاضی حداقل یک بار حضورا به یکی از نمایندگان مراجعه کرده و پس از تنظیم اسناد لازم ، کلیدرمز خود را رسما تحویل می گیرد.
- از آن لحظه به بعد مسئولیت حفظ و نگهداری از کلید خصوصی یا کلید مشترک را بر عهده دارد؛
- اگر کلید از یکی از طرفین سرقت شود یا گم شود مجددا باید این فرایند تکرار شود.
- این روش در بسیاری از محیط ها جوابگو نخواهد بود.

الگوریتم مبادله دیفی هلمن

- به عنوان مثال برای ثبت نام از راه دور و ایجاد حساب کاربری از راه دور هیچگاه نمی توان افراد را حضورا برای تحویل کلید دعوت کرد بلکه بایستی از طریق همین خطوط ناامن ، کلید رمز افراد را به آن ها تحویل داد.
- حال تصور کنید که وقتی کلید رمز برای اولین و آخرین بار مسیر ناامن شبکه را طی می کند ، استراق سمع شود. سرقت کلید رمز مساوی است با ناامنی مطلق زیرا تمام داده های رمزشده توسط فرستنده ، برای نفوذگری که کلید رمز را دزدیده قابل بهره برداری است.
- لذا روش ایجاد کلید سرّی بین طرفین یک ارتباط، از سال ها قبل مورد توجه پژوهشگران این فن بوده است.

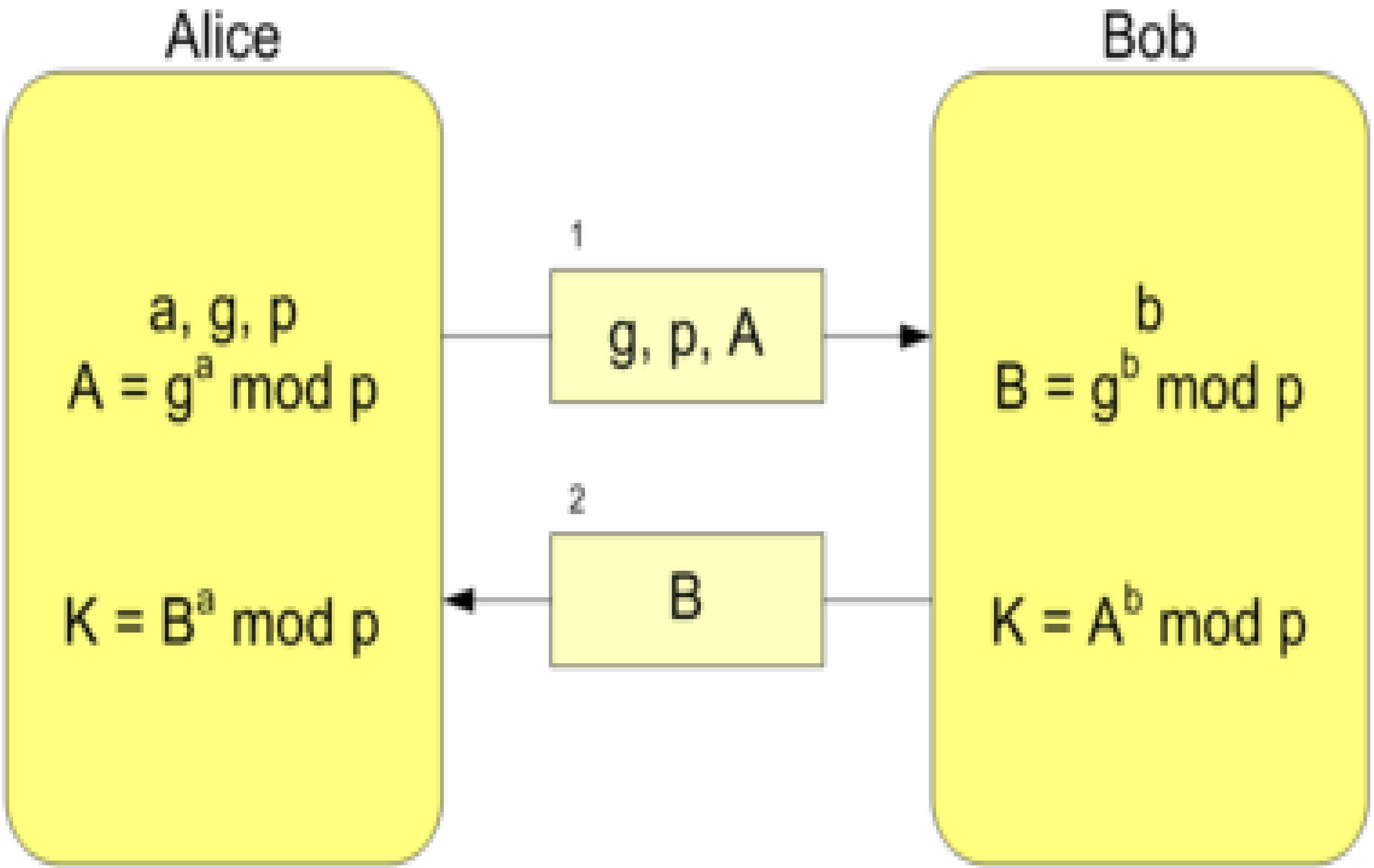
الگوریتم مبادله دیفی هلمن

- درسال 1977 دو پژوهشگر جوان به نامهای ویتفیلد دیفی و مارتین هلمن الگوریتمی برای ایجاد و توافق برروی یک کلید ابداع و آن را به نام خود ثبت کرده اند.
- البته شخص سومی هم در این میانه به نام رالف مرکل وجود داشت که جزو بنیادگذاران روش به حساب می آید ولی گویا تاریخ به این اسم وفادار نبوده و الگوریتم به نام دیفی – هلمن در اذهان تثبیت شده است.
- این الگوریتم تحت عنوان یک اختراع با شماره

US PATENT 4,200,770

به ثبت رسید ولی اعتبار آن حدود ده سال پیش منقضی شده و استفاده عمومی از آن آزاد است.

الگوریتم دیفی –هلمن نیز براساس دشواری محاسبه لگاریتم گسسته بنا نهاده شده است.



$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$$

الگوریتم مبادله دیفی هلمن

در شکل قبل الیس میخواهد با باب بر روی کلیدی توافق کند تا برای رمزنگاری اطلاعات در آینده از آن استفاده نماید.

روال کار:

1. الیس یک عدد اول بسیار بزرگ انتخاب و آن را P می نامد. (انتخاب P به روش جستجو انجام میگیرد)
2. الیس یکی از مولدهای میدان Z(P) را انتخاب کرده وآن را g می نامند. پیداکردن g که به روش جستجو و آزمون انجام می گیرد ، چندان دشوار نیست .
3. الیس یک عدد دلخواه و محرمانه انتخاب کرده و نزد خود نگاه می دارد. این عدد سری است و هرگز بر روی خط ارسال نخواهد شد ؛ این عدد را a فرض کنید.

الگوریتم مبادله دیفی هلمن

- 4. الیس A رابه صورت زیر محاسبه میکند :
- $A=(g^a) \bmod p$

5. سه تایی (g,p,A) برای باب ارسال می شود و استراق سمع شدن آن توسط افراد بیگانه اهمیتی ندارد.

6. با دریافت سه تایی (g,p,A) ؛ باب بلافاصله یک عدد تصادفی بزرگ انتخاب کرده و آن را b می نامند . این عدد هم سری است ونزد باب نگهداری می شود . $B=(g^b) \bmod p$

7. باب B را برای آلیس پس می فرستد.

8. باب برای بدست آوردن کلید سری و مشترک با الیس ، عدد A را در پیمانه P به توان b (عدد سری خودش) می رساند:

$$K=(A^b) \bmod p =(g^a)^b \bmod p = g^{a.b} \bmod p$$

الگوریتم مبادله دیفی هلمن

- 9. الیس نیز برای محاسبه کلید سری و مشترک با باب ، عدد B را در پیمانه P به توان a (عدد سری خودش) می رساند:
- $K=(B^a) \mod p =(g^b)^a \mod p = g^{a.b} \mod p$
- در حقیقت طبق الگوریتم بالا کلیدی ایجاد می شود که نیمی ازآن پیشنهاد آلیس و نیم دیگر متعلق به باب است.
- حال چطور یک بیگانه قادر به محاسبه کلید مشترک آلیس وباب نیست.

آنکه یک بیگانه قادر به استراق سمع آن است عبارت است از اعداد p,g,A,B و برای بدست آوردن کلید مشترک یا باید A را به توان b(عدد سری باب) یا آنکه عدد B را به توان a (عدد سری آلیس) برساند که هیچکدام از این دو (a,b) را در اختیار ندارد. از آنجا که هیچ رابطه ی سرراست ومستقیمی برای محاسبه لگاریتم گسسته وجود ندارد تلاش او برای یافتن a از طریق A یا b از طریق B بی حاصل خواهد بود

زیرا : $A=(g^a) \mod p$

$B=(g^b) \mod p$

الگوریتم مبادله دیفی هلمن

- مثال:
- الف) آلیس به عنوان شروع کننده عدد p=23 را به عنوان پیمانه محاسبات انتخاب می کند

. این میدان به تعداد (22) Q معادل ده ریشه ی اولیه (مولد) دارد

که عبارتند از اعداد

5و7و10و11و14و15و17و19و20و21

- ب)الیس از بین این ده مولد فرضا g=5 را به عنوان عدد دلخواه درنظرمیگیرد
- ج) الیس عدد سری خود را a=6 فرض کرده واز طریق آن A را به صورت زیر محاسبه می کند:

الگوریتم مبادله دیفی هلمن

$A=(g^a) \bmod p = 5^6 \bmod 23 = 8$

- د) حال الیس سه تایی را به صورت (8و23و5) برای باب می فرستد.
- ه) به طریق مشابه باب با انتخاب عددتصادفی b=15 محاسبه زیر را انجام می دهد:

$B=(g^b) \bmod p = 5^{15} \bmod 23 = 19$

و) عدد B به الیس برگشت داده می شود (B =19)

ز) باب کلید سری و مشترک خود را به صورت زیر محاسبه می کند:

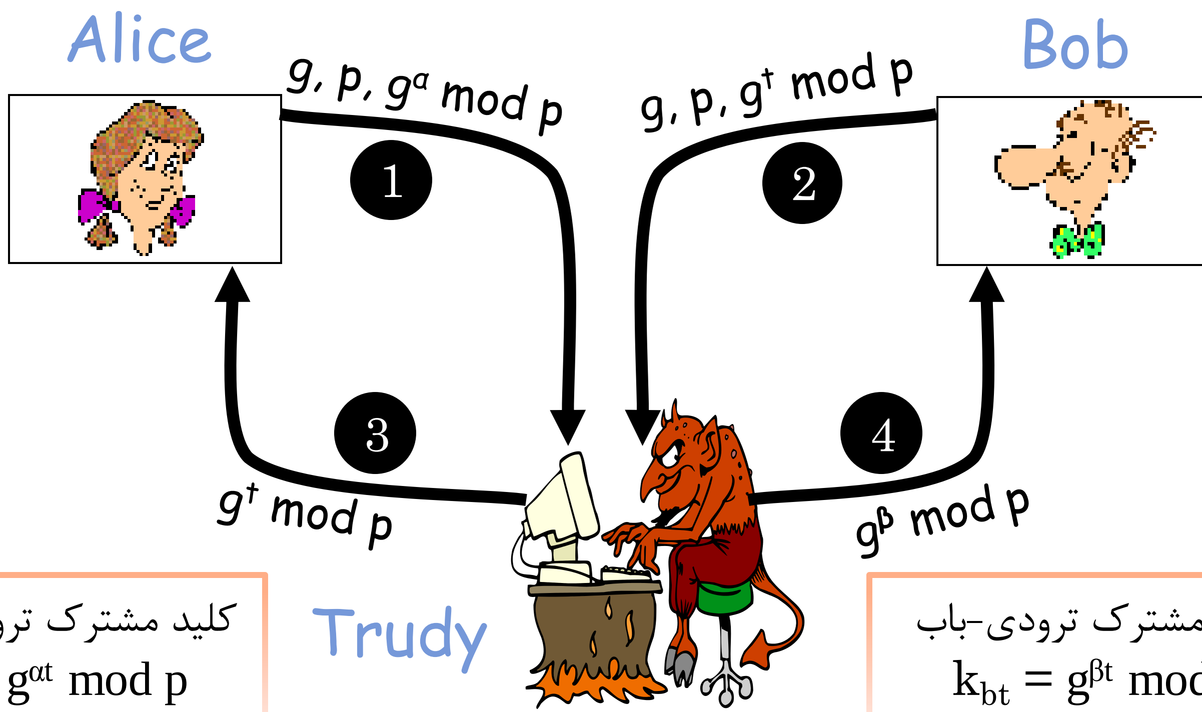
$K=(A^b) \bmod p = 8^{15} \bmod 23 = 2$

ح) الیس نیز با محاسبه K به همین کلید خواهد رسید :

$K=(B^a) \bmod p = 19^6 \bmod 23 = 2$

حمله شخص میانی علیه الگوریتم دیفی - هلمن

- مشکل اصلی : حمله مرد میانی



کلید مشترک ترودی-آلیس
$k_{at} = g^{\alpha t} \bmod p$

کلید مشترک ترودی-باب
$k_{bt} = g^{\beta t} \bmod p$