Shahid Beheshti University

رمزنگاری

هادی سلیمانی

پژوهشکده فضای مجازی دانشگاه شهید بهشتی

مجوز استفاده و نشر

- اجازه‌ی ایجاد نسخه‌های دیجیتالی جدید براساس بخشی یا تمام مطالب این اسلاید بدون پرداخت هزینه اعطا می‌شود، مشروط بر این‌که:
  - فقط به‌منظور و در راستای استفاده‌ی آموزشی (شخصی و یا کلاسی) ساخته شده باشند و برای کسب هرگونه سود و یا مزیت تجاری استفاده نشوند.
  - نسخه‌های جدید حاوی ارجاع مستقیم به نام تهیه‌کننده اسلاید (هادی سلیمانی) و محل کار وی (پژوهشکده فضای مجازی دانشگاه شهید بهشتی) باشند.
- مجموعه‌ی حاضر براساس نظرات ارزشمند دانشجویان (سابق) دانشگاه شهید بهشتی و همکاران محترم تهیه شده است که از تمام آن‌ها قدردانی می‌شود؛

  (به‌خصوص خانم‌ها **سارا زارعی** و **فاطمه عزیزی** نقش مهمی را در تهیه نسخه‌ی نهایی بر عهده داشته‌اند. خانم مهندس زارعی علاوه بر کمک در آماده‌سازی نسخه‌ی فعلی اسلایدها، در تصحیح اشتباهات نسخه‌ی قبلی و همچنین تکمیل و بازتعریف محتوای درس‌ها بسیار تاثیرگذار بوده‌اند).
- برای مشاهده‌ی اسلایدها و ویدئوهای تدریس این درس به آدرس زیر مراجعه فرمایید:

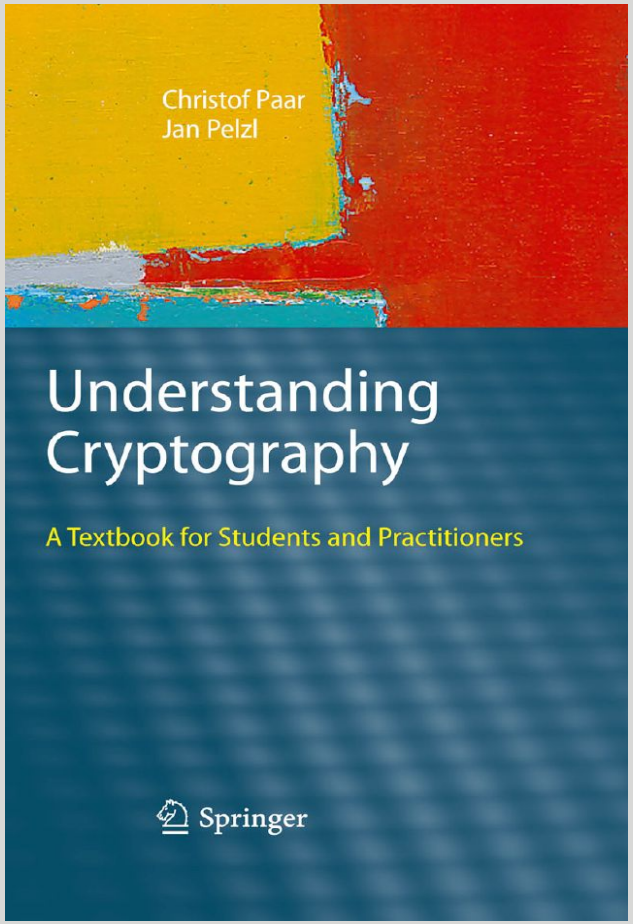
http://facultymembers.sbu.ac.ir/h_soleimany/cryptography-course/

درس یازدهم

رمزنگاری کلید عمومی مبتنی بر لگاریتم گسسته

معرفی مـرجع

رمزنگاری کلید عمومی مبتنی بر لگاریتم گسسته



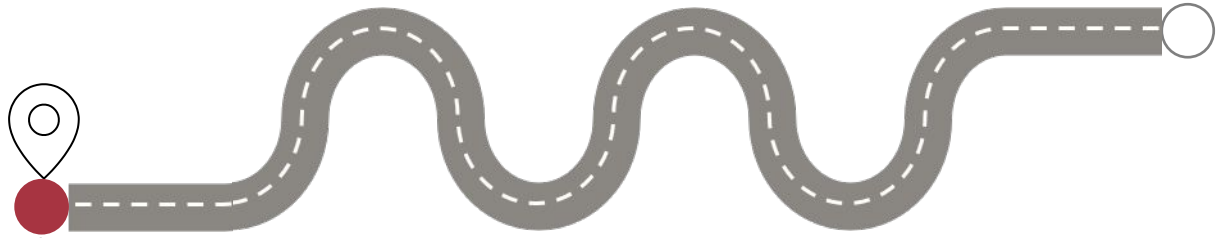
Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.

مثال‌ها و تصاویر این بخش از درس از کتاب مرجع است (در غیر این صورت مرجع شکل ذکر شده است).

فهرست عناوین درس

رمزنگاری کلید عمومی مبتنی بر لگاریتم گسسته

- مقدمه
- توافق کلید دفی ـ هلمن
- رمزنگاری الجمال
- امنیت الجمال
- روش‌های حل لگاریتم گسسته
- جمع‌بندی مطالب



مقدمه

مرتبه‌ی گروه و عضو

(یادآوری)

- **مرتبه‌ی گروه**

تعداد اعضای یک گروه محدود را مرتبه‌ی گروه گوییم.

- **مرتبه‌ی عضو**

اگر k کوچک‌ترین عددی باشد که $\alpha^k = e$ (e عضو همانی است)، در این صورت k را مرتبه‌ی α گوییم.

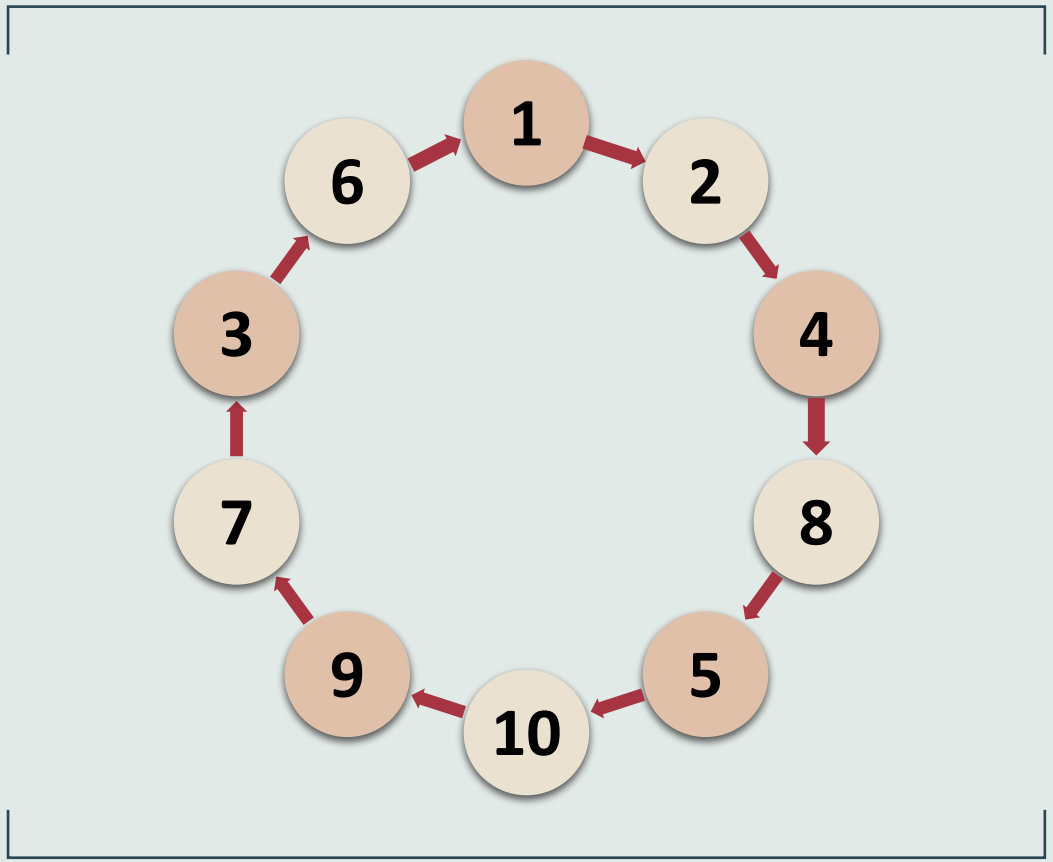
- **قضیه‌ی لاگرانژ:**

1. مرتبه‌ی هر زیرگروه، مرتبه‌ی گروه را می‌شمارد.
2. مرتبه‌ی هر عضو، مرتبه‌ی گروه را می‌شمارد.

گروه دوری

(یادآوری)

- اگر G یک گروه باشد و $\alpha \in G$، آن‌گاه
$$\langle \alpha \rangle = \{\alpha^n | n \in \mathbb{Z}\}$$
یک زیرگروه G است که زیرگروه دوری تولیدشده توسط α نامیده می‌شود.
- گروه G را یک گروه دوری گوییم هرگاه یک عنصر مانند $\alpha \in G$ وجود داشته باشد به‌نحوی‌که: $\langle \alpha \rangle = G$.
- دراین صورت α را مولد G می‌گوییم.
- مثال: $\mathbb{Z}_{11}^*$ را نسبت به عمل ضرب پیمانه‌ای و پایه‌ی 2 در نظر می‌گیریم:



$$\langle \alpha \rangle = G$$

مسئله‌ی لگاریتم گسسته

- مسئله‌ی لگاریتم گسسته: برای گروه متناهی و دوری G به همراه عملگر $*$، دو عضو $\alpha,\beta \in G$ داده شده‌اند که α مولد گروه است. مقدار $0 \leq d \leq |G| - 1$ را پیدا کنید به نحوی که رابطه‌ی زیر صادق باشد:

$$\beta = \underbrace{\alpha * \alpha * \cdots * \alpha}_{d \text{ مرتبه}} = \alpha^d$$

سختی مسئله‌ی لگاریتم گسسته

- مسئله‌ی لگاریتم گسسته در تمامی گروه‌ها یک مسئله‌ی سخت نیست.
- مثلا در گروه $G = (\mathbb{Z}_p, +)$ مقدار لگاریتم گسسته با استفاده از الگوریتم توسعه یافته اقلیدسی به راحتی قابل محاسبه است:

$$d.\alpha = \beta \bmod p \Rightarrow d = \alpha^{-1}.\beta \bmod p$$

- مسئله‌ی لگاریتم گسسته در برخی گروه‌ها نظیر $\mathbb{Z}_p^*$، $\mathbb{Z}_{2^n}^*$ و خم‌های بیضوی بسیار سخت است.
- از آن‌جایی‌که سختی مسئله‌ی لگاریتم گسسته در گروه ضربی $\mathbb{Z}_{2^n}^*$ نسبت به گروه ضربی $\mathbb{Z}_p^*$ کمتر است، در کاربردهای رمزنگاری عموما از $\mathbb{Z}_{2^n}^*$ استفاده نمی‌شود.
- دراین درس تمرکز ما بر روی گروه ضربی $\mathbb{Z}_p^*$ خواهد بود و درس بعدی (درس ۱۲ام) با خم‌های بیضوی آشنا خواهیم شد.

مسئله‌ی لگاریتم گسسته در Z_p^*

- مسئله‌ی لگاریتم گسسته در Z_p^*: دو عضو $\alpha,\beta \in Z_p^*$ داده شده‌اند. p یک عدد اول است و مرتبه‌ی α برابر $p-1$ است. مقدار $0 \leq d \leq p-1$ را پیدا کنید به نحوی که رابطه‌ی زیر صادق باشد:

$$\beta = \alpha^d \bmod p$$

- اصطلاحا d را لگاریتم گسسته β در پایه‌ی α می‌نامند و به صورت زیر نمایش می‌دهند:

$$d = \log_\alpha \beta \bmod p$$

- از آنجایی‌که مسئله‌ی لگاریتم گسسته در Z_p^* یک مسئله‌ی سخت است، تابع توان‌رسانی پیمانه‌ای یک‌طرفه است و بنابراین مناسب استفاده در رمزنگاری است.
- سوال: چگونه می‌توان برای گروه $\mathbb{Z}_p^*$ که p یک عدد اول است، عضو α را انتخاب کرد به نحوی که مرتبه‌ی α، عدد بزرگی باشد؟

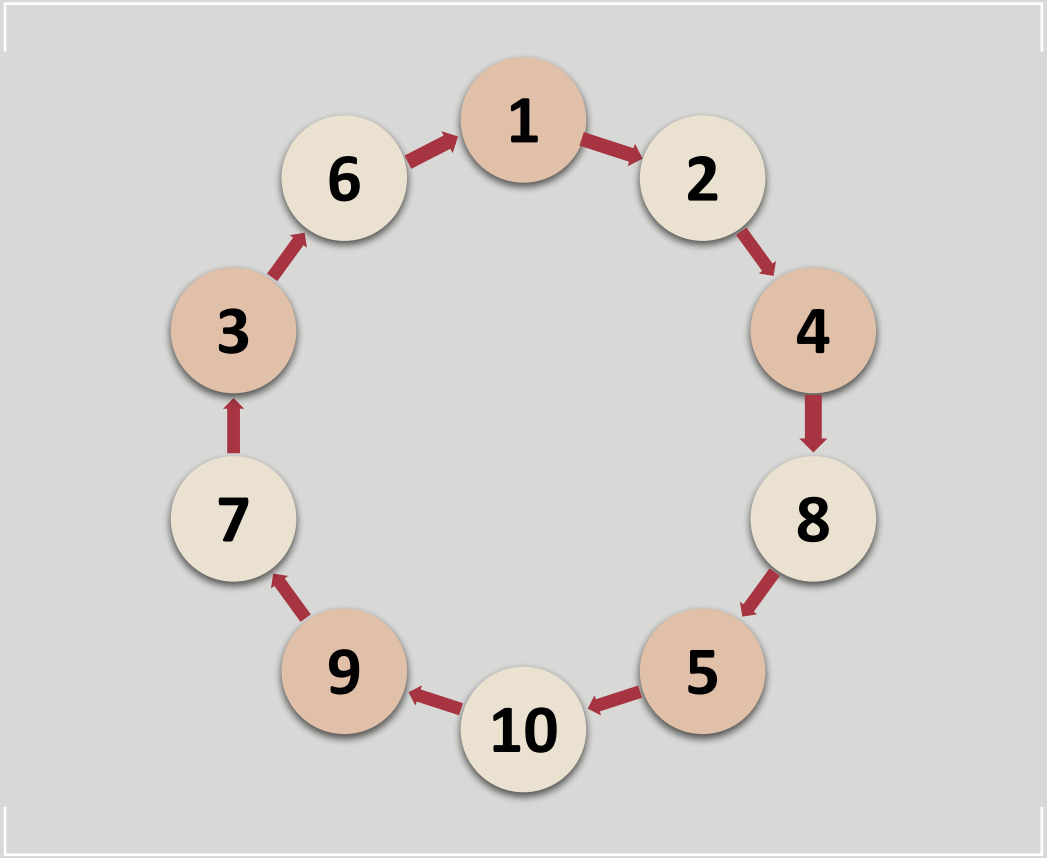
راهکار عملی برای انتخاب مناسب پارامترها

مثال

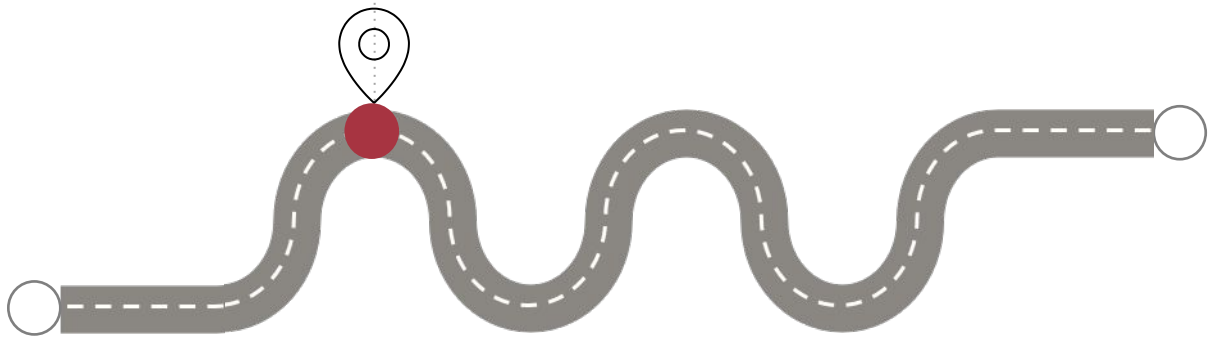
- می‌خواهیم مرتبه 2 در گروه $\mathbb{Z}_{11}^*$ نسبت به عمل ضرب پیمانه‌ای را محاسبه کنیم.
- براساس قضیه لاگرانژ می‌دانیم $ord(2)|10$.
- مرتبه‌ی هر عضو (غیر از 1)، 2 یا 5 و یا 10 است.
- برای پیدا کردن مرتبه‌ی 2 لازم نیست که تمامی مقادیر را امتحان کرد!

$$2^2 \equiv 4 \bmod 11$$
$$2^5 \equiv 32 \equiv 10 \bmod 11$$

- بنابراین بدون هیچ محاسبه‌ی اضافی دیگر، می‌توان نتیجه گرفت که مرتبه‌ی 2 برابر است با 10.



توافق کلید
دفی - هلمن



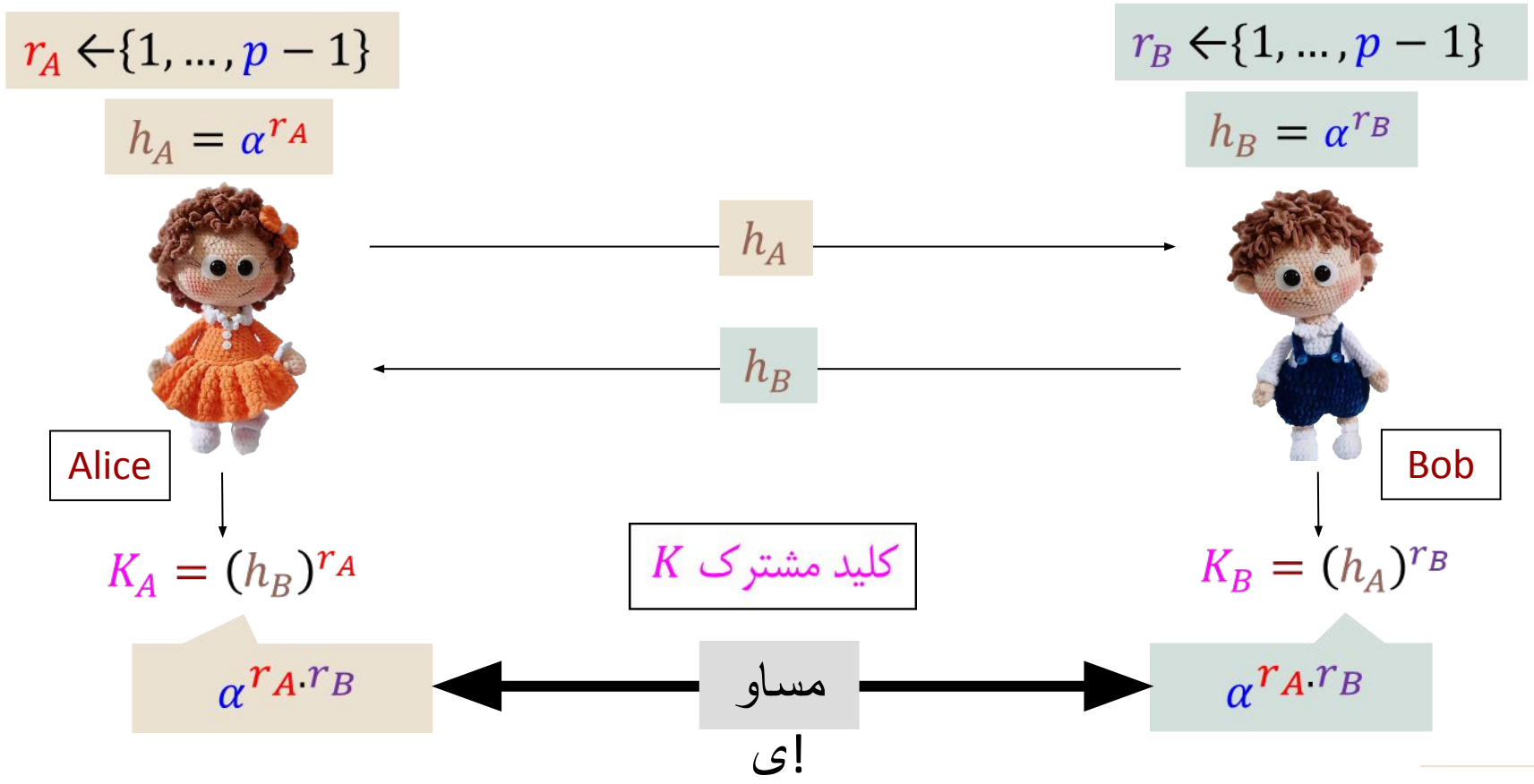
مقدمه

استقرار کلید

- در هر سیستم رمزنگاری نیاز است که به نحوی کلید(ها) تولید و در اختیار طرفین قرار بگیرد که در درس 16 به تفصیل در این خصوص صحبت خواهیم کرد.
- انتقال کلید: کلید توسط یک طرف تولید و به صورت امن برای طرف دیگر ارسال می‌کند.
- طرح توافق کلید، یک پروتکل تعاملی (Interactive) است که در آن دو کاربر بر روی یک کلید توافق می‌کنند، بدون آن‌که به حضور یک شخص سوم مورد اعتماد نیاز باشد.

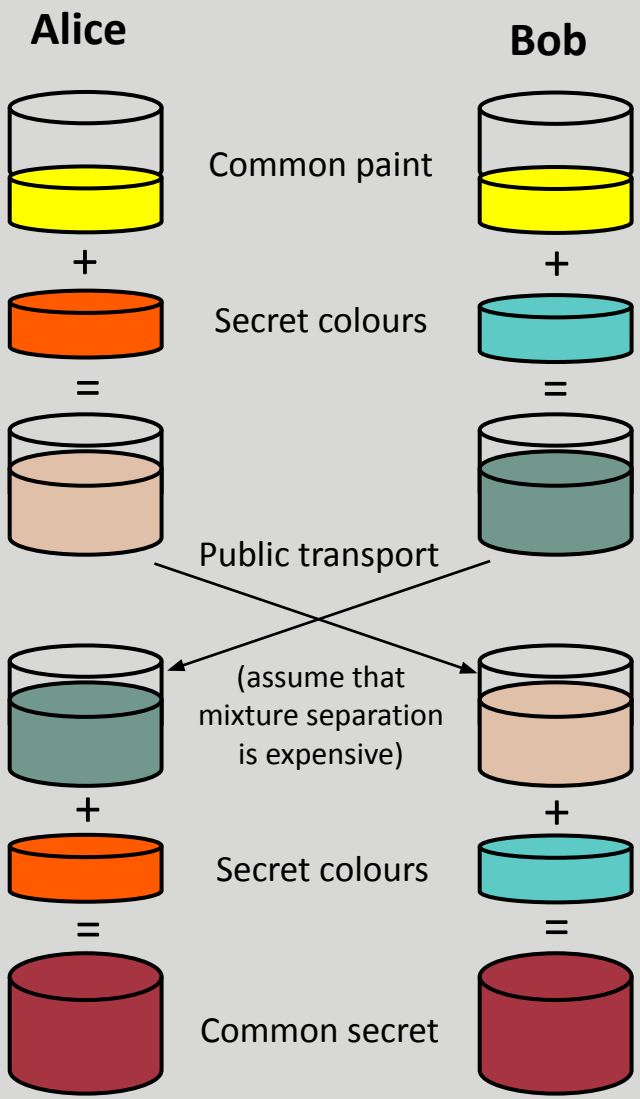
طرح توافق کلید دفی ـ هلمن

- گروه G با مجموعه‌ی $\mathbb{Z}_p^*$ و عمل ضرب پیمانه‌ای را در نظر می‌گیریم.
- عضو α به‌گونه‌ای که $G = \langle \alpha \rangle$ را نیز به عنوان پایه در نظر می‌گیریم.



تشبیهی از نحوه‌ی عملکرد پروتکل دفی ـ هلمن

- برای تقریب به ذهن، می‌توان کارکرد پروتکل دفی – هلمن را با یک مثال ساده توصیف کرد.
- فرض کنید در ابتدا هر یک از دو کاربر دارای یک رنگ مشترک و عمومی در ظرف‌های شیشه‌ای خود هستند (α).
- سپس هر کاربر یک رنگ دلخواه و مخفی را نیز برای خود انتخاب کرده (r_A , r_B) و با رنگ اولیه ترکیب می‌کند تا رنگ جدید تولید شود (h_A ,h_B).
- ظرف‌های شیشه‌ای از طریق حمل و نقل عمومی (در مقابل چشم همه) بین طرفین مبادله می‌شوند.
- هر یک از طرفین رنگ مخفی خود را به ظرف دریافتی از طرف مقابل اضافه می‌کند و هر دو در نهایت یک رنگ مشترک خواهند داشت (کلید مشترک K).



A.J. Han Vinck, Introduction to public key cryptography, p. 16

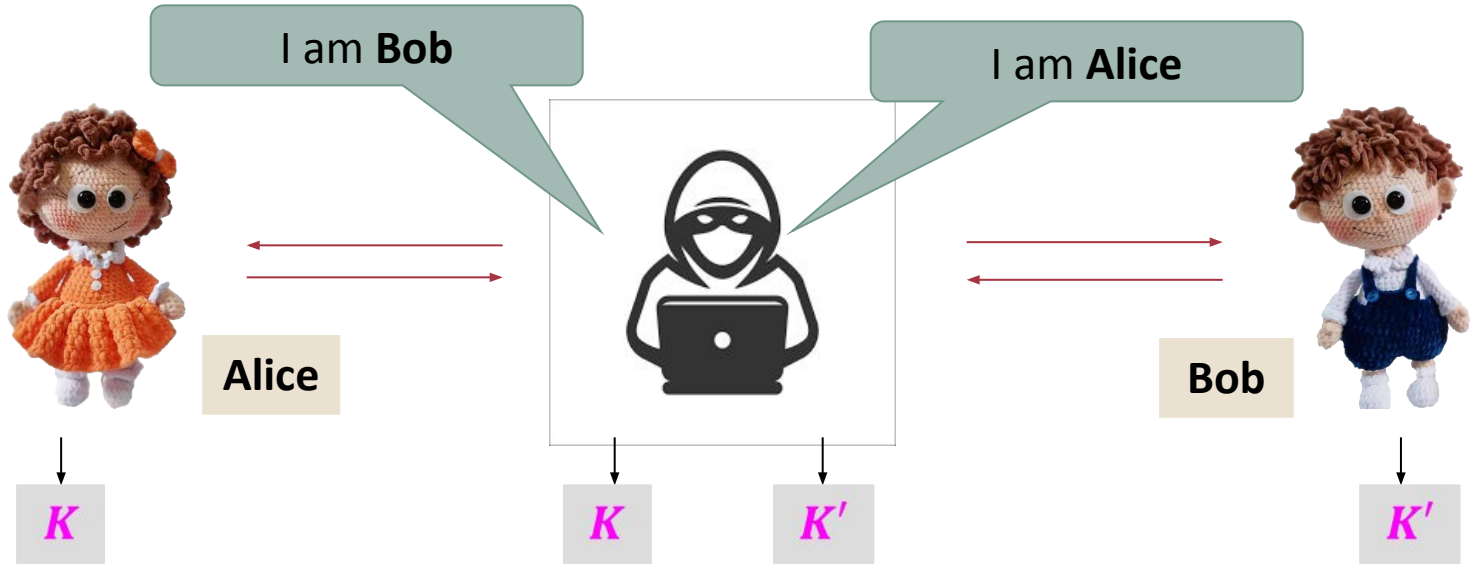
امنیت توافق کلید دفی ـ هلمن

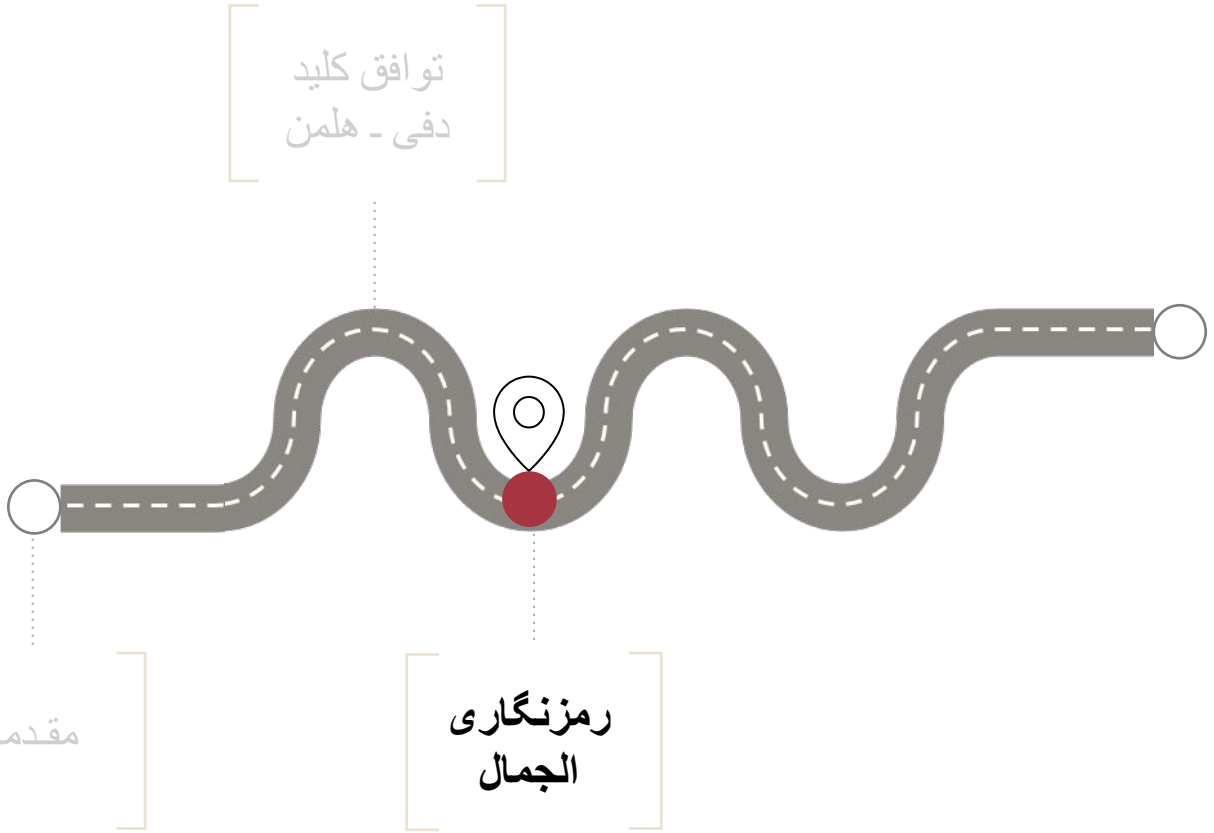
- بدیهی است که اگر مسئله‌ی لگاریتم گسسته قابل حل باشد، پروتکل توافق کلید دفی ـ هلمن امن نیست.
- به منظور امن بودن سیستم، مهاجم نباید بتواند مقادیر r_A و r_B را با مشاهده‌ی h_A و h_B محاسبه کند.
  1. مرتبه‌ی گروه انتخابی باید به اندازه‌ی کافی بزرگ باشد (یعنی p).
  2. مرتبه‌ی عضو انتخابی باید به اندازه‌ی کافی بزرگ باشد (یعنی $ord(\alpha)$).
- مسئله‌ی Computational Diffie–Hellman: با داشتن مقادیر $(\alpha,\alpha^{r_A},\alpha^{r_B})$ بتوان مقدار $K = \alpha^{r_A.r_B}$ را محاسبه کرد.
- تاکنون هیچ حمله‌ای که توسط مهاجم غیرفعال قابل اعمال باشد ارائه نشده است.

حمله‌ی مردی در میانه

(Man-in-the-Middle Attack)

- برای آلیس و باب مشخص نیست که طرف مقابل واقعا چه کسی است!
- مهاجم فعال می‌تواند هر کدام از طرفین را فریب بدهد!
- حمله‌ی بسیار کاربردی و مهمی است.
- تبادل کلید دفی ـ هلمن در عمل با اعمال یک سری تغییرات (با هدف افزودن احراز اصالت طرفین مقابل) استفاده می‌شود.




توافق کلید
دفی ـ هلمن
مقدمه
رمزنگاری
الجمال

تولید کلیدها رمزنگاری الجمال

- عدد اول قوی (و بزرگ) p انتخاب می‌شود.
- یک عضو اولیه (مولد) α در گروه $(\mathbb{Z}_p^*, \times)$ انتخاب می‌شود.
- کلید خصوصی $d \in \{2, \dots, p-1\}$ به صورت تصادفی تولید می‌شود.
- مقدار β به صورت $\beta = \alpha^d \pmod p$ محاسبه می‌شود.
- مقادیر (α, β, p) به عنوان کلید عمومی اعلام عمومی می‌شوند.
- مقدار d به عنوان کلید خصوصی به صورت مخفی نگهداری می‌شود.

سیستم رمزنگاری الجمال

(ElGamal)

عملیات رمزگذاری

یک مقدار تصادفی i را تولید کرده سپس پیام m را به صورت زیر رمز می‌کنیم:

$$E(m,i) = (y_1, y_2)$$

که در آن: $y_1 = \alpha^i \bmod p$ و $y_2 = m\beta^i \bmod p$

عملیات رمزگشایی

$$m = D(y_1, y_2) = y_2 . (y_1^d)^{-1} \bmod p$$

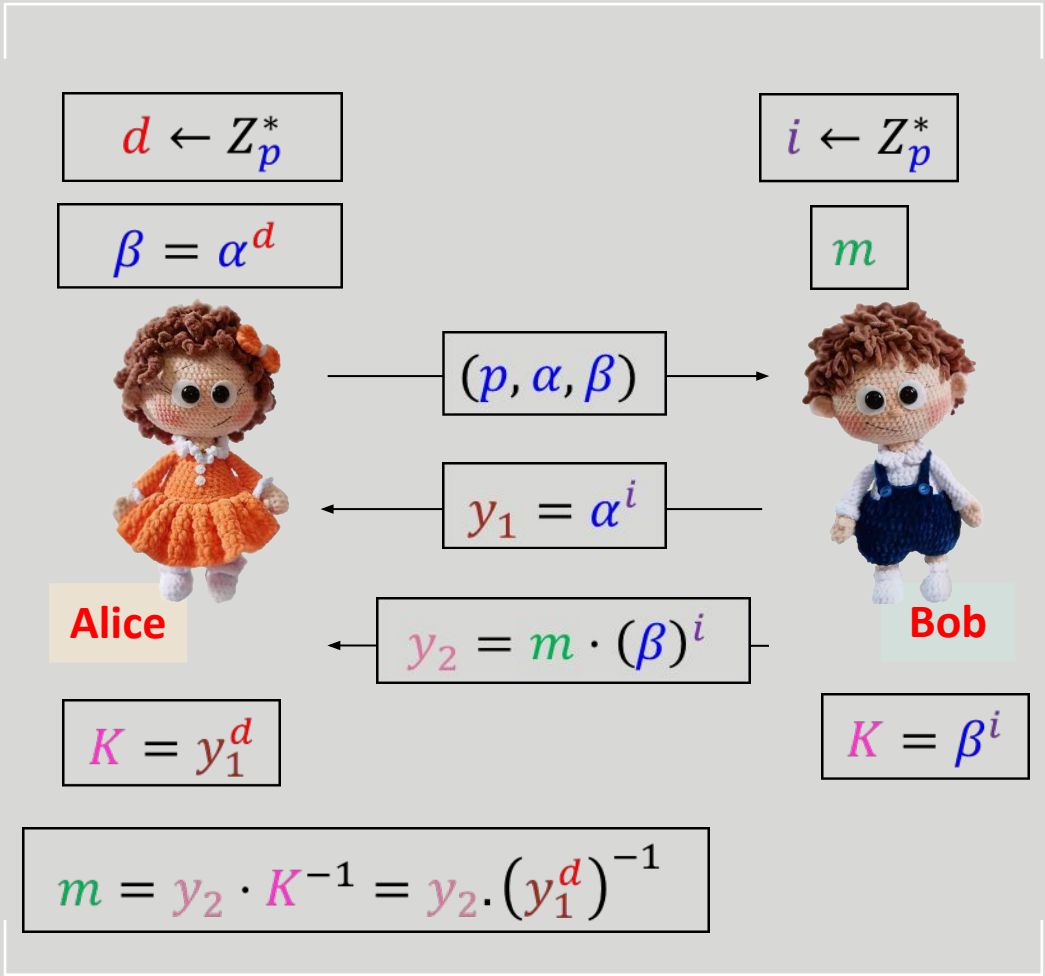
اثبات صحت رمزگشایی:

$$y_2 . (y_1^d)^{-1} \bmod p$$
$$= m\beta^i . \alpha^{-i.d} =$$
$$m(\alpha^d)^i . \alpha^{-i.d}$$
$$= m$$

سیستم رمزنگاری الجمال از نگاهی دیگر

توافق کلید دفی ـ هلمن

- آلیس مقدار $\beta = \alpha^d$ را محاسبه کرده و در اختیار همه (از جمله باب) قرار می‌دهد.
- باب مقدار $y_1 = \alpha^i$ را محاسبه کرده و آن را روی کانال ناامن برای آلیس ارسال می‌کند.
- کلید مشترک بین آلیس و باب، همانند توافق کلید دفی ـ هلمن برابر با $K = \alpha^{i.d}$ است.
- کلید K برای باب به صورت $K = \beta^i$ قابل محاسبه است.
- کلید K برای آلیس به صورت $K = y_1^d$ قابل محاسبه است.



رمزگذاری:

$$y_2 = m \cdot K = m.\beta^i$$

رمزگشایی:

$$m = c \cdot K^{-1} = y_2.(y_1^d)^{-1}$$

سیستم رمزنگاری الجمال

مثال

- کلید خصوصی: $d = 12$
- کلید عمومی: $(p = 29, \quad \alpha = 2, \quad \beta = 2^{12} \bmod 29 = 7)$
- عملیات رمزگذاری $m = 26$ با در نظر گرفتن عدد تصادفی $i = 5$

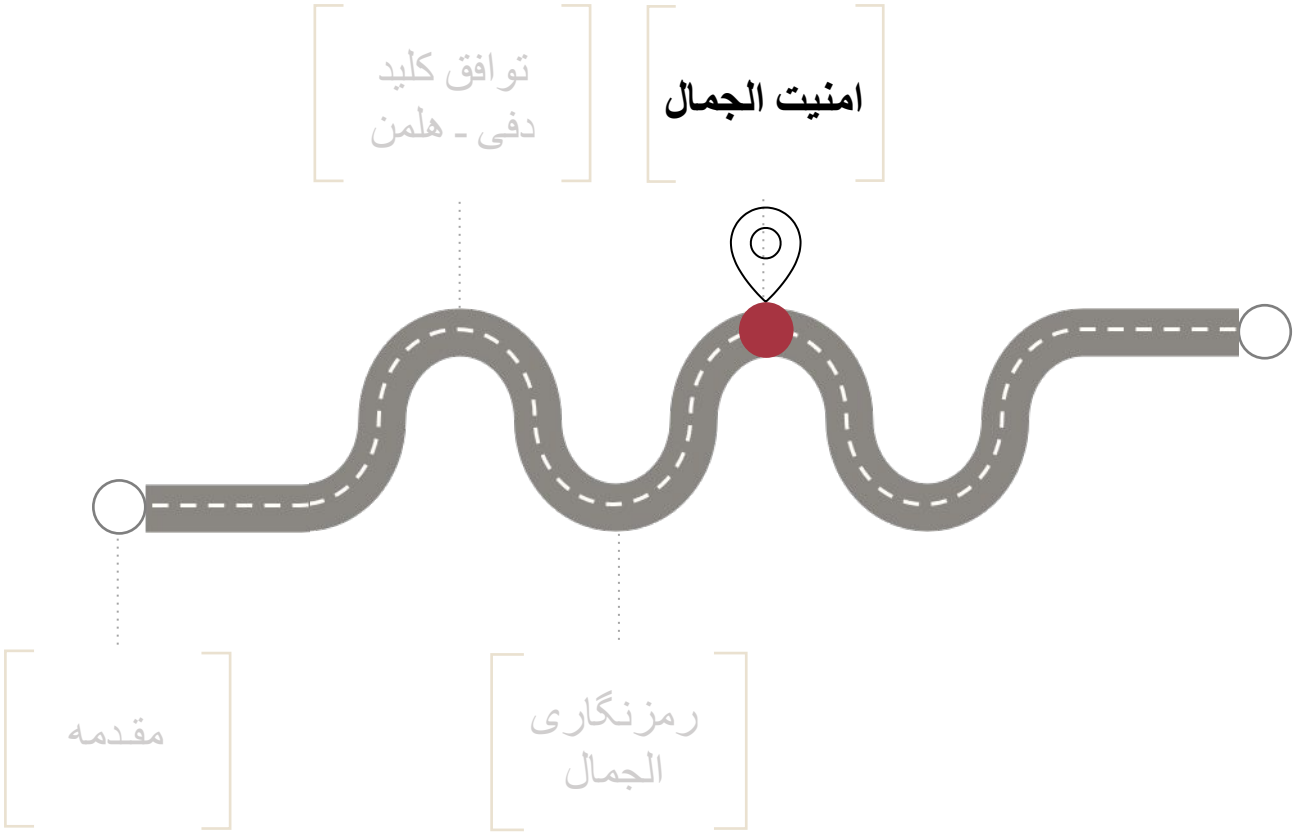
$$y_1 = \alpha^i \bmod p = 2^5 \bmod 29 = 3$$

$$y_2 = m\beta^i \bmod p = 26 \times 7^5 \bmod 29 = 10$$

- عملیات رمزگشایی:

$$y_1^d = 3^{12} \bmod 29 = 16$$

$$m = 16^{-1} \times y_2 = 20 \times 10 = 26 \bmod 29$$


توافق کلید
دفی ـ هلمن
امنیت الجمال
مقدمه
رمزنگاری
الجمال

خاصیت هم‌ریختی

- رمزنگاری الجمال نسبت به عمل ضرب خاصیت هم‌ریختی دارد، یعنی:

ضرب دو متن رمز شده‌ی $\mathrm{Enc}_{pk}(m) = (y_1, y_2)$ و $\mathrm{Enc}_{pk}(m') = (y_1', y_2')$، معادل متن رمزشده‌ی $m.m'$ است.

- **اثبات:**

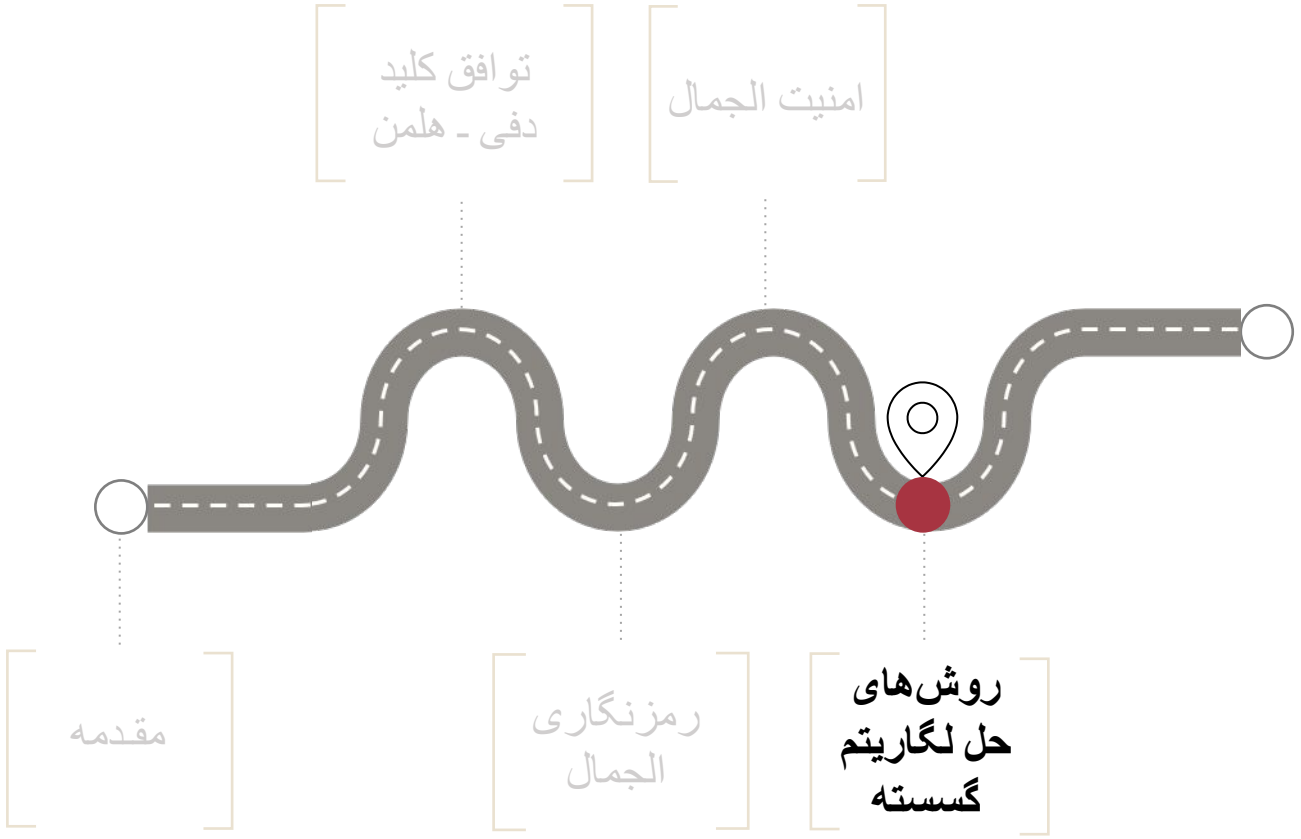
$$\mathrm{Enc}_{pk}(m) = (y_1, y_2) = (\alpha^i \bmod p, m\beta^i \bmod p)$$
$$\mathrm{Enc}_{pk}(m') = (y_1', y_2') = (\alpha^{i'} \bmod p, m'\beta^{i'} \bmod p)$$
$$(y_1.y_1', y_2.y_2') = (\alpha^i.\alpha^{i'} \bmod p, m\beta^i.m'\beta^{i'} \bmod p)$$
$$= (\alpha^{i+i'} \bmod p, m.m'\beta^{i+i'} \bmod p)$$

که برابر با معادل رمزشده‌ی متن $m.m'$ است (با مقدار تصادفی معادل $i + i'$).

خاصیت هم‌ریختی

... ادامه

- احتمال استفاده از ویژگی هم‌ریختی در بسیار از کاربردهای عملی توسط مهاجم بسیار پایین است.
- به خاطر نقش مقدار تصادفی، هر متن اصلی در دو عملیات رمزگذاری متفاوت به متن رمزشده‌های مختلفی تبدیل می‌شود.
- بنابراین برخی از ضعف‌هایی که نسخه‌ی کتابی RSA دارد را الجمال نداشته و نیازی به اضافه کردن عامل تصادفی ندارد.


توافق کلید
دفی ـ هلمن
امنیت الجمال
مقدمه
رمزنگاری
الجمال
روش‌های
حل لگاریتم
گسسته

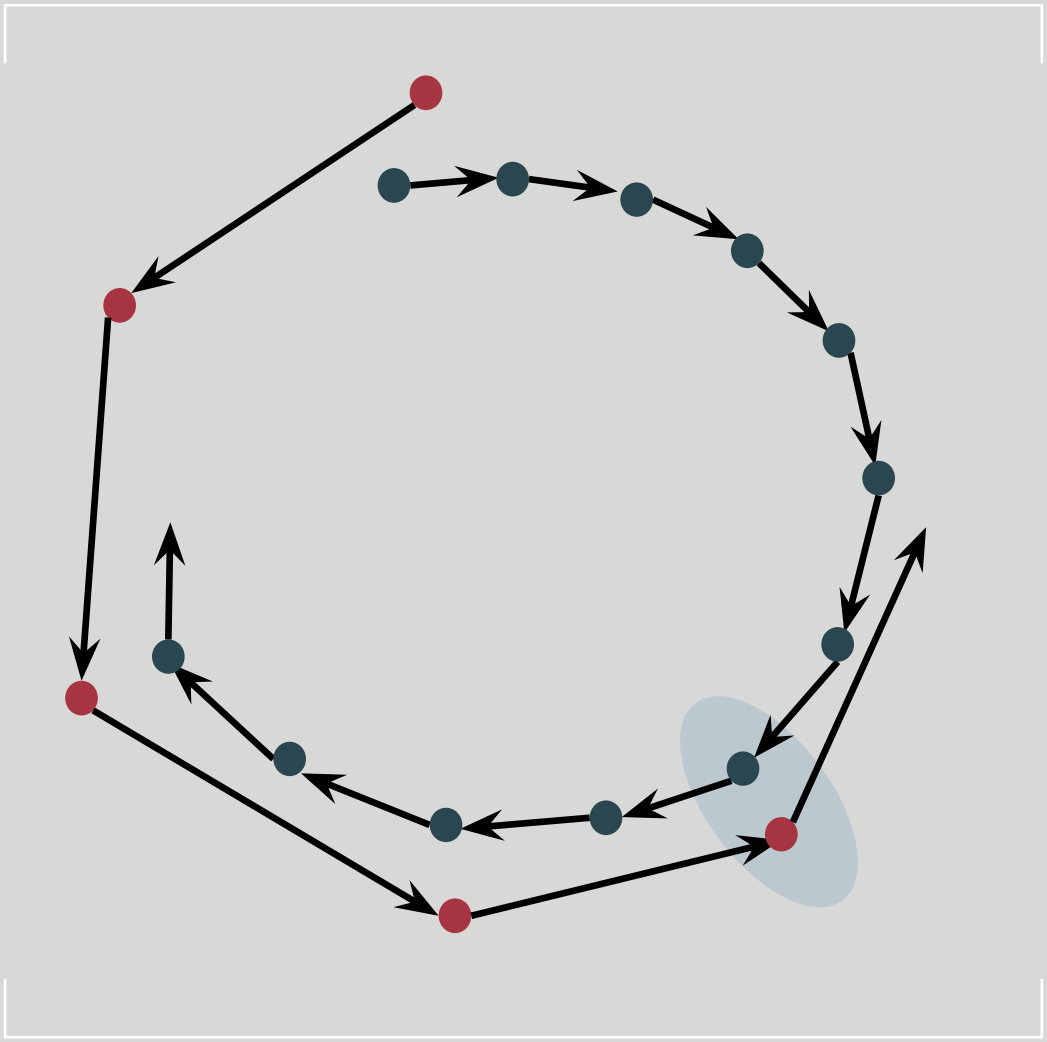
جست‌وجوی کامل

- صورت مسئله: گروه دوری $G = \langle \alpha \rangle$ با مرتبه‌ی n را در نظر می‌گیریم.
- فرض کنید $\beta \in G$ داده شده است. می‌خواهیم x را به صورتی پیدا کنیم که:

$$\beta = \alpha^x$$

- به ازای تمام مقادیر $1 \leq i \leq n$ مقدار α^i را محاسبه کرده و چک می‌کنیم که آیا برابر با β می‌شود یا خیر.
- زمان مورد نیاز از مرتبه‌ی $O(n)$ است.
- برای گروه دوری که شامل اعضای $\mathbb{Z}_p^*$ با عمل ضرب پیمانه‌ای است، پیچیدگی از مرتبه‌ی $O(2^{|p|})$ است.

الگوریتم Shank



- براساس قضیه‌ی تقسیم، مقدار x را می‌توان به شکل یکتا به صورت $x = Nx_b + x_g$ نمایش داد که $N = \lceil \sqrt{n} \rceil$.
- مقادیر x_b و x_g را می‌توان به‌صورت مستقل با روش زیر پیدا کرد:

1. مقدار $\alpha^{N.x_b}$ را به ازای مقادیر $0 \le x_b \le N$ محاسبه و ذخیره می‌کنیم (موسوم به Baby Step).
2. به ازای $0 \le x_g \le N$، مقدار $\beta.\alpha^{-x_g}$ را محاسبه می‌کنیم (موسوم به Giant Step).

اگر با یکی از مقادیر مجموعه‌ی گام اول برابر شد، مقدار x بازیابی می‌شود:

$$\alpha^{N.x_b} = \beta.\alpha^{x_g} \implies x = Nx_b + x_g$$

- زمان مورد نیاز و همچنین حافظه از مرتبه $O(\sqrt{n})$ است.
- برای گروه دوری $\mathbb{Z}_p^*$، پیچیدگی از مرتبه‌ی $O(2^{|p|/2})$ است.

Figure's source: "Introduction to Information Security" Course by Kwangjo Kim

روش Pollard's Rho

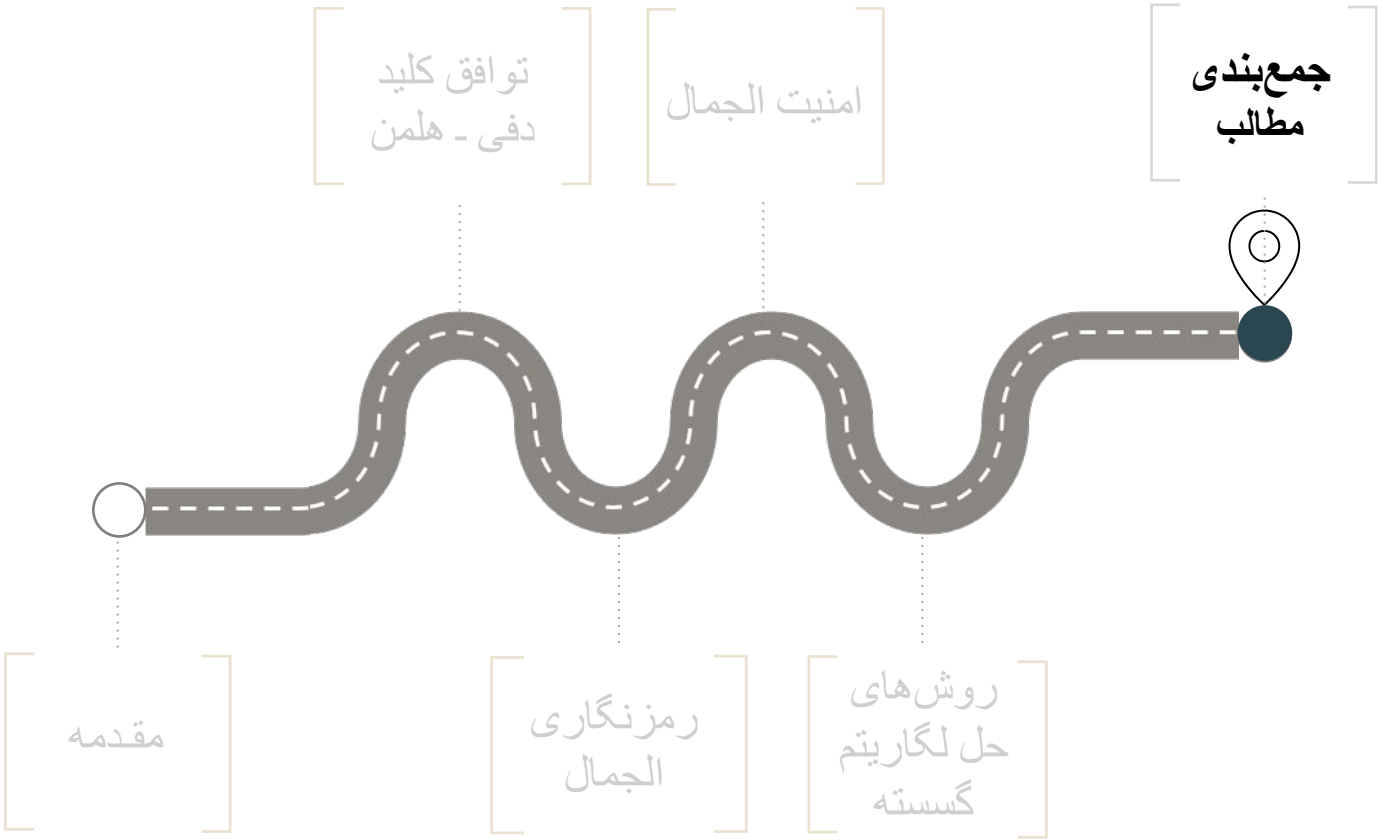
- ایده‌ی کلی این است که به صورت تصادفی مقادیری به شکل $\alpha^i.\beta^j$ تولید کرده و دنباله را به صورت موثر ذخیره کنیم.
- با یافتن یک تصادم داریم:

$$\alpha^{i_1}.\beta^{j_1} = \alpha^{i_2}.\beta^{j_2} \Rightarrow \alpha^{i_1}.(\alpha^x)^{j_1} = \alpha^{i_2}.(\alpha^x)^{j_2}$$
$$\alpha^{i_1+x.j_1} = \alpha^{i_2+x.j_2} \Rightarrow i_1 + x.j_1 = i_2 + x.j_2$$
$$x = \frac{i_2 - i_1}{j_1 - j_2}$$

- یکی از بهترین الگوریتم‌های شناخته‌شده برای حل لگاریتم گسسته است.
- زمان اجرا از مرتبه $O(\sqrt{n})$ است و حافظه‌ی مورد نیاز بسیار محدود است.
- **نتیجه**: برای داشتن امنیت k بیت، مرتبه گروه (n) باید حداقل 2^{2k} باشد (این نتیجه برای هر گروهی صادق است).

روش Index-Calculus

- این روش صرفا مختص برخی گروه‌های دوری نظیر $\mathbb{Z}_p^*$ است و به یک گروه در حالت عمومی قابل اعمال نیست.
- روش بسیار موثری است، به‌نحوی‌که برای داشتن ۸۰ بیت امنیت باید عدد اول انتخابی برای $\mathbb{Z}_p^*$ حداقل ۱۰۲۴ بیت باشد.
- این مسئله موجب شده است که سیستم‌های کلید عمومیِ مبتنی بر مسئله‌ی لگاریتم گسسته در گروه‌های دیگر مورد توجه بیشتری قرار بگیرند.
- در درس بعدی (درس دوازدهم) با خم‌های بیضوی و تعریف مسئله لگاریتم گسسته بر روی آن‌ها آشنا خواهیم شد.
- رمزنگاری مبتنی بر خم بیضوی نیاز به طول کلید کوتاه‌تری دارد.


جمع‌بندی مطالب
امنیت الجمال
توافق کلید دفی ـ هلمن
روش‌های حل لگاریتم گسسته
رمزنگاری الجمال
مقدمه

جمع‌بندی مطالب

- اولین طرح کلید عمومی ارائه‌شده مبتنی بر مسئله‌ی لگاریتم گسسته است (طرح توافق کلید دفی ـ هلمن).
- طرح توافق کلید دفی ـ هلمن بسیار کارا است و امروزه به صورت گسترده به‌کارمی‌رود.
- طرح رمزنگاری الجمال که مبتنی بر مسئله‌ی لگاریتم گسسته است در نرم‌افزارهای بسیار پرکاربرد پیاده‌سازی شده و به‌کارمی‌رود.
- به منظور درک گستردگی استفاده از سیستم های رمزنگاری کلید عمومی کافی است که بدانیم هر مرورگر اینترنتی (Web Browser) از یک سیستم رمزنگاری مبتنی بر لگاریتم گسسته استفاده می‌کند.
- مسئله‌ی لگاریتم گسسته در برخی گروه‌های دیگر نیز سخت است و می‌توان آن را به صورت مشابه بازتعریف کرد (در درس بعدی خواهیم دید).