آشنایی با رمزنگاری

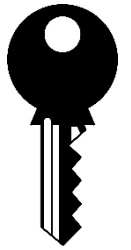
کلید عمومی

علیرضا شاولی

شروع مسئله‌دار

- باب هدیه‌ای برای آلیس خریده ولی با توجه به 

نمی‌تواند شخصاً هدیه را به او بدهد.
  - بنابراین مجبور است از طریق پست ارسال کند.
- متاسفانه در سرزمین عجایب همه‌ی پستچی‌ها دزد هستند!
  - نامه‌ها را می‌خوانند
  - محتویات بسته‌های بدون قفل را می‌دزدند
- آیا باب هیچ راهی دارد؟



حل مسئله

- اسلاید قبلی خیلی مسئله‌دار است.
  - چه معنی دارد که باب برای آلیس هدیه بفرستد!
  - اصلاً چه معنی دارد ما از این اسامی بیگانه استفاده کنیم!
- راه‌حل: بومی‌سازی
  - باب ⟵ فرهاد آلیس ⟵ شیرین

حل مسئله

- اسلاید قبلی خیلی مسئله‌دار است.
  - چه معنی دارد که باب برای آلیس هدیه بفرستد!
  - اصلاً چه معنی دارد ما از این اسامی بیگانه استفاده کنیم!
- راه‌حل: بومی‌سازی
  - باب ← فرهاد آلیس ← شیرین
- حالا بگویید چه کند بیچاره فرهاد؟

حل مسئله

- اسلاید قبلی خیلی مسئله‌دار است.
  - چه معنی دارد که باب برای آلیس هدیه بفرستد!
  - اصلاً چه معنی دارد ما از این اسامی بیگانه استفاده کنیم!
- راه‌حل: بومی‌سازی
  - باب ⟵ فرهاد آلیس ⟵ شیرین
- حالا بگویید چه کند بیچاره فرهاد؟

حل مسئله

- اسلاید قبلی خیلی مسئله‌دار است.
  - چه معنی دارد که باب برای آلیس هدیه بفرستد!
  - اصلاً چه معنی دارد ما از این اسامی بیگانه استفاده کنیم!
- راه‌حل: بومی‌سازی
  - باب ⟵ فرهاد آلیس ⟵ شیرین
- حالا بگویید چه کند بیچاره فرهاد؟

در باب نامه نوشتن فرهاد، شیرین را

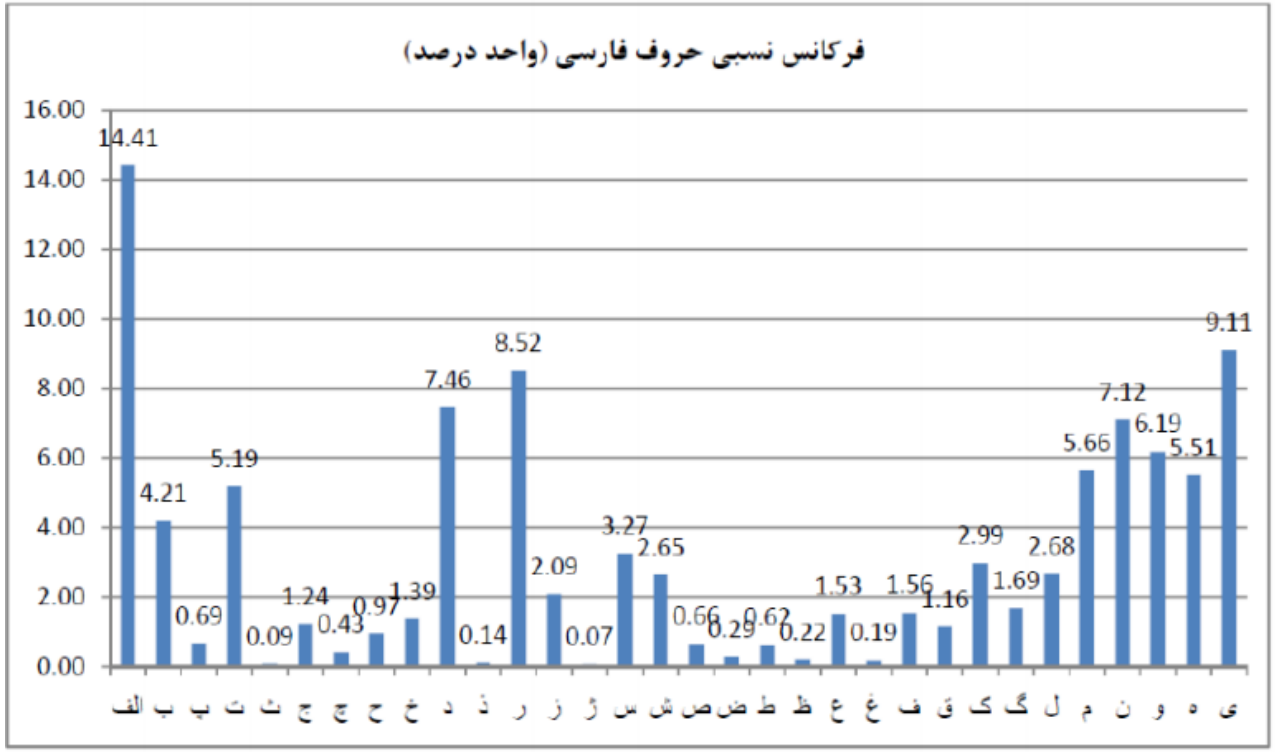
- حال فرض کنید فرهاد می‌خواهد نامه‌ای برای شیرین بفرستد. ولی
  - همه‌ی پست‌چی‌ها جاسوسان خسرو هستند
- فرهاد مجبور است رمزی بنویسید
  - طوری که شیرین بفهمد
  - و خسرو نفهمد
- به نظر شما فرهاد بی‌نوا باید چه کند؟
  - یک رومی پاسخ می‌دهد!

مردی به نام ژولیو

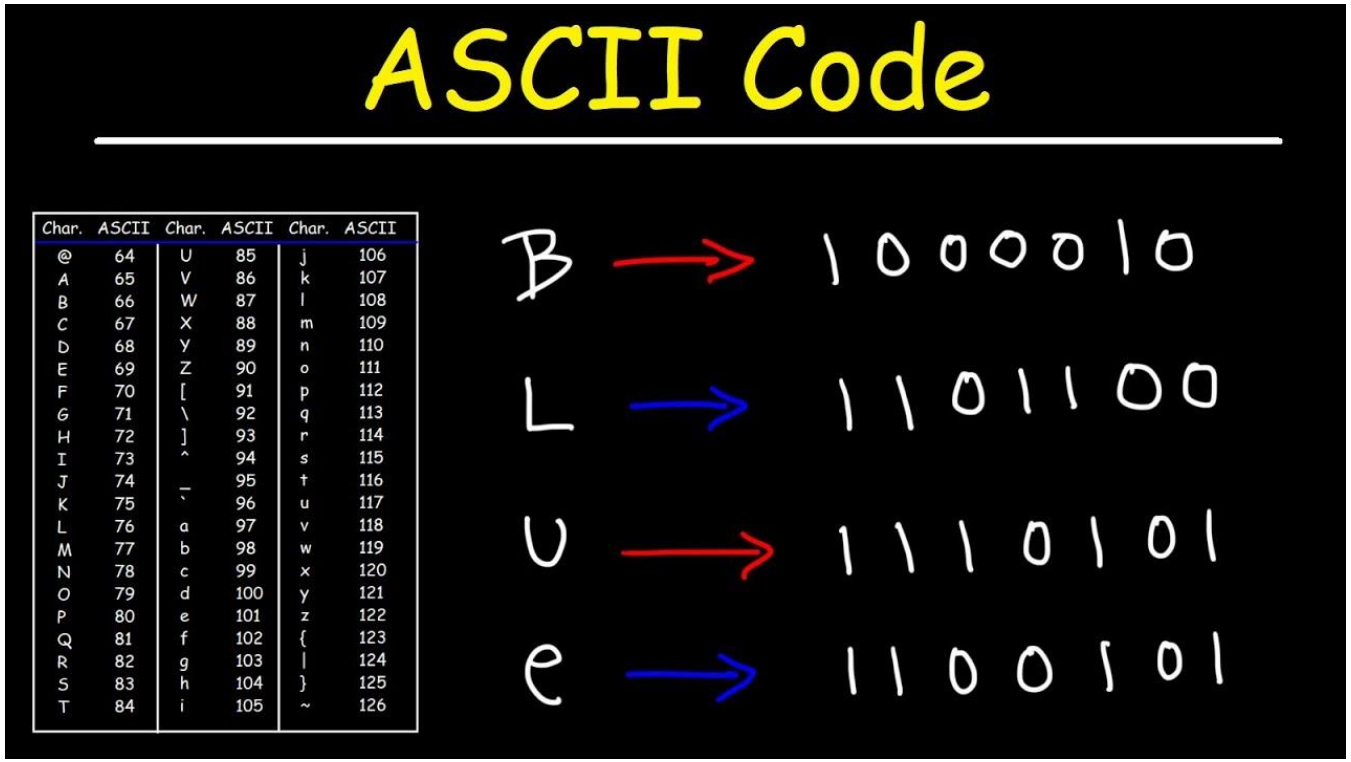
- ژولیو سزار و کدهای انتقالی
- آ ← پ ب ← ت پ ← ث ...
- به نظر شما کدهای سزار چقدر امن بودند؟
- تعمیم: کدهای جایگشتی
- به نظر شما کدها جایگشتی چقدر امن هستند؟

مردی به نام ابویوسف یعقوب بن اسحاق بن الصّبّاح بن عمران بن اسماعیل بن محمد بن أشعث بن قیس الکِنْدی

- ابویوسف الکندی و تحلیل بسامد



رمزنگاری کلید خصوصی



- گام صفر: تبدیل کردن نامه به عدد!
  - کد ASCII
- مثال: BLUE

1000010110110011101011100101

رمزنگاری کلید خصوصی (ادامه)

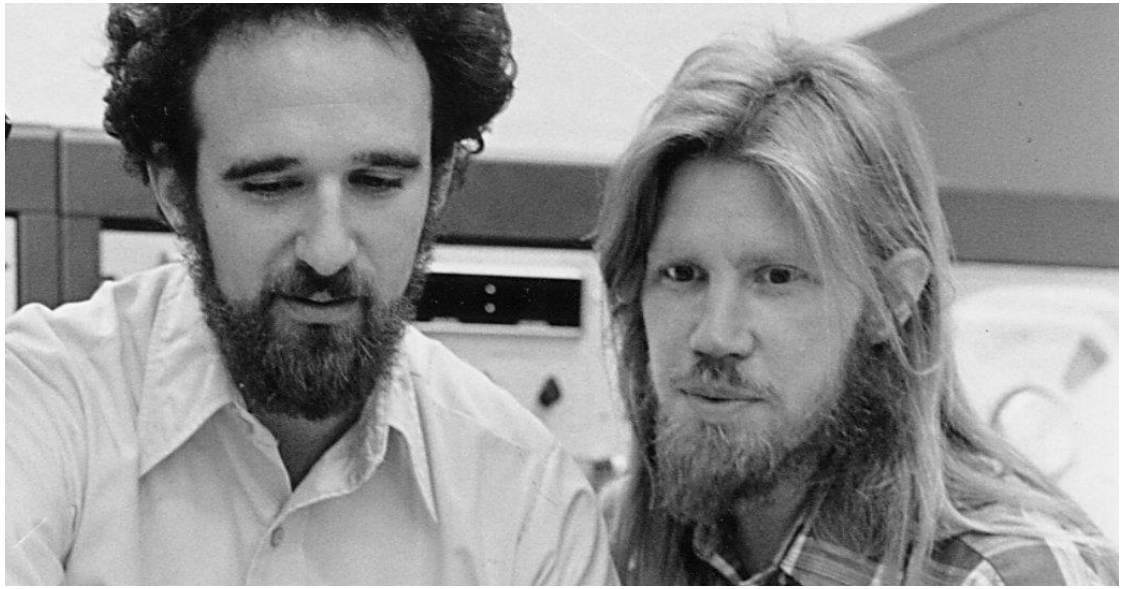
- گام یک: توافق پنهانی!
  - عددی مشترک (کلید خصوصی): 489930883788497329910878939834 1
- از این پس فرض می‌کنیم نامه‌ی فرهاد عدد m و کلید خصوصی عدد k است.
- گام دو: نوشتن نامه
  - فرهاد برای شیرین می‌نویسد mk
- گام سه: خواندن نامه
  - شیرین نامه را بر k تقسیم می‌کند

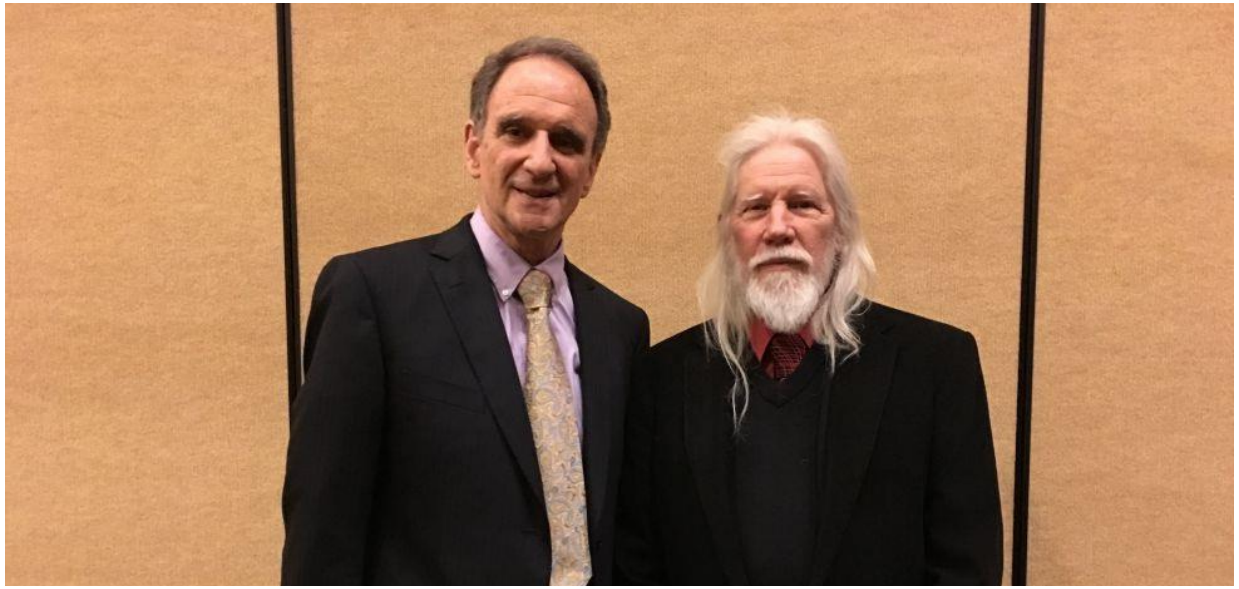
زندگی سخت است!

- راه حل قبلی در عمل در بسیاری موارد قابل اجرا نیست.
  - فرهاد فرصت توافق پنهانی را نداشته.
  - امروزه در ارتباطات ما تعیین کردن کلید خصوصی از قبل ممکن است مشکل باشد.
  - در برخی شرایط اصلاً ناممکن است، مثلاً جنگ.
- باید به دنبال روش جدیدی باشیم.
  - رمزنگاری کلید عمومی: این اصلاً با عقل جور در می‌آید؟

تولد رمزنگاری کلید عمومی

- در سال ۱۹۷۶، ویتفیلد دیفی و مارتین هلمن مشکل فرهاد را حل کردند.
  - آن‌ها راهی برای ساختن یک کلید خصوصی مشترک پیدا کردند که نیازی به ارتباطی خارج از کانال اصلی ندارد.





- البته ظاهراً حقیقت این است که رمزنگاری کلید عمومی در جنگ جهانی دوم متولد شده‌است.

اشتراک کلید دیفی- هلمن

فرهاد

خسرو

شیرین

کارهای شیرین:

- دریافت عدد اول p
- دریافت عدد g
- انتخاب عدد خصوصی $s < p$
- محاسبه g^s به پیمانه‌ی p و ارسال
- دریافت باقیمانده‌ی g^f بر p
- محاسبه‌ی کلید مشترک: g^{fs} بر p

داده‌های خسرو:

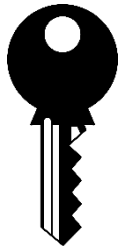
- عدد اول p
- عدد g
- باقیمانده g^f بر p
- باقیمانده g^s بر p

کارهای فرهاد:

- انتخاب عدد اول بزرگ p و ارسال
- انتخاب g نه لزوماً بزرگ و ارسال
- انتخاب عدد خصوصی $f < p$
- محاسبه g^f به پیمانه‌ی p و ارسال
- دریافت باقیمانده‌ی g^s بر p
- محاسبه‌ی کلید مشترک: g^{sf} بر p

سختش نکنیم؟

- چرا اینقدر پیچاندیمش؟
  - به توان رساندن، محاسبه باقیمانده و ...
  - نمی‌شد عملیات‌های ساده‌تری انتخاب کرد، مثلاً ضرب به جای توان؟
- بعد از انتخاب s و f فرض کنید:
  - شیرین gs را برای فرهاد بفرستد
  - فرهاد gf را برای شیرین بفرستد
  - و بعد هر دو gfs را حساب کنند
- داده‌های خسرو: g, gs, gf
  - با یک تقسیم ساده (به پیمانه‌ی p) f و s را حساب می‌کند
  - پس کلید مشترک gfs را هم می‌تواند حساب کند

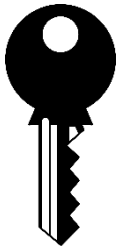


نکته کجاست؟

- پس فرق روش دیفی-هلمن در چیست؟
  - چرا مشکل روش اسلاید قبل را ندارد؟
- تفاوت در این است که:
  - تقسیم به پیمانه‌ی p ساده بود
  - لگاریتم به پیمانه‌ی p ساده نیست!
- مثال: فرض کنید $g = 2$ و $p = 23$ و خسرو (به پیمانه 23) $2^f \equiv 3$ را می‌بیند.
  - خسرو برای یافتن f باید همه حالت‌ها را چک کند.
  - در واقعیت با p خیلی بزرگ‌تری سر و کار داریم

$$2^{?} \equiv 719635999 \quad (\text{به پیمانه } 1872023093)$$

مسئلهٔ



$$2^{1012} \equiv 719635999 \quad (\text{به پیمانه } 1872023093)$$

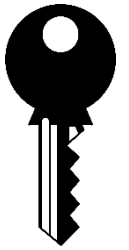
- دیدیم یافتن پاسخ برای خسرو سخت است
  - باید باقیمانده‌ی همه‌ی توان‌ها را حساب کند
  - ولی آیا این محاسبه برای فرهاد همین قدر سخت نیست؟
- روشی برای محاسبه‌ی سریع توان: نوشتن توان در مبنای ۲

$$1012 = (1111110100)_2 = 512 + 256 + 128 + 64 + 32 + 16 + 4$$

- بنابراین داشتن 2 به توان توان‌های 2 کافیست:

$$2^{16} = 65536 \Rightarrow 2^{32} \equiv 550921110 \Rightarrow 2^{64} \equiv 90962788$$

$$\Rightarrow 2^{128} \equiv 923081617 \Rightarrow 2^{256} \equiv 1586548832 \Rightarrow 2^{512} \equiv 1112412805$$



انتقال پیام بدون اشتراک کلید

- یک سال بعد از ارائه‌ی الگوریتم دیفی- هلمن الگوریتم رمزنگاری RSA ارائه شد.
  - این الگوریتم نیازی به اشتراک کلید ندارد
- قضیه‌ی اویلر: اگر p,q دو عدد اول متمایز باشند و a عددی صحیح که بر آن‌ها بخش‌پذیر نیست آنگاه:

$$a^{(p-1)(q-1)} \equiv 1 \ (\text{به پیمانه } pq)$$

- نتیجه: برای محاسبه‌ی باقیمانده‌ی a^n بر pq کافیست اول باقیمانده‌ی n بر $(p-1)(q-1)$ را حساب کنید و اگر این باقیمانده r باشد، باقیمانده a^n بر pq با باقیمانده‌ی a^r یکی است.
- مثال: باقیمانده‌ی 3^{50} بر 35 چقدر است؟
  - راه‌حل: $35 = 5 \times 7$ پس $(5-1) \times (7-1) = 24$. پس باقیمانده‌ی 3^{24} و نیز 3^{48} بر 35 برابر ۱ است.
  - پس باقیمانده‌ی 3^{50} بر 35 برابر 9 است.

الگوریتم RSA

فرهاد

خسرو

شیرین

کارهای شیرین:

- انتخاب دو عدد اول بزرگ p,q و ارسال $n = pq$
- انتخاب عدد s که نسبت به $(p-1)(q-1)$ اول
- ارسال s به فرهاد
- دریافت باقیمانده‌ی a^s بر n
- محاسبه‌ی وارون ضربی s به پیمانه $(p-1)(q-1)$
- محاسبه‌ی $(a^s)^{s^*} \equiv a^{ss^*} \equiv a \ (mod\ n)$

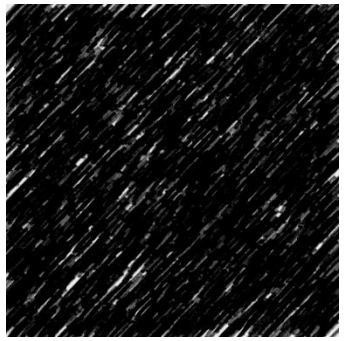
داده‌های خسرو:

- عدد $n = pq$
- عدد s
- باقیمانده‌ی a^s بر n

کارهای فرهاد:

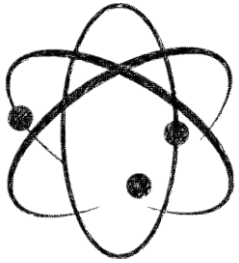
- دریافت n و s
- تبدیل کردن نامه به عدد $a < n$
- محاسبه‌ی باقیمانده‌ی a^s بر n و ارسال آن

به چه کار آید این که می‌گویی؟



- تبادل محرمانه اطلاعات در موقعیت‌های حساس
  - جنگ
  - عملیات‌های اطلاعاتی
- انتقال داده‌های مهم در بستر اینترنت
  - بانکداری الکترونیکی
  - پروتکل SSL (الگوریتم RSA و دیفی- هلمن خم بیضوی)
- ارتباطات امن در بستر اینترنت
  - تلگرام
  - کاربر-سرور
  - کاربر-کاربر

کوانتوم



- کوانتوم را به ما چه کار؟
  - کامپیوترهای کوانتومی
- الگوریتم شور و محاسبه‌ی مرتبه در زمان چندجمله‌ای
  - حل سریع مسئله‌ی تجزیه
  - محاسبه‌ی سریع لگاریتم گسسته
- رمزنگاری پساکوانتوم
  - نامه‌ی وزارت دفاع آمریکا
  - مشبکه مبنا: NTRU
  - هم‌ذاتی مبنا: SIDH

سوال

خسته نباشید