دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)
دانشکدهٔ مهندسی کامپیوتر و فنآوری اطلاعات

مبانی امنیت اطلاعات

(ترم بهمن ۹۸)

Diffie-Hellman

نستوه طاهری جوان

nastooh@aut.ac.ir

پروتکل Diffie-Hellman

نیاز اصلی الگوریتم های رمزنگاری متقارن:

کلید مشترک و سری

- الگوریتم های رمزنگاری متقارن، بر این فرض استوارند که دو طرف، یک کلید یکسان و محرمانه در اختیار دارند.
  - کلیدی که بین دو طرف ارتباط مشترک بوده، اما دیگران از آن اطلاع ندارند.
  - تبادل آن از طریق شبکه، موجب استراق سمع آن می شود.
  - یک راه، استفاده از یک شبکه دیگر (امن) برای تبادل کلید است.
    - مثلا: تبادل کلید به کمک تلفن!، نامه!، کبوتر!، تحویل دستی! و سپس استفاده از این کلید در رمزنگاری متقارن در شبکهٔ نا امن...
- اما سوال مهم:

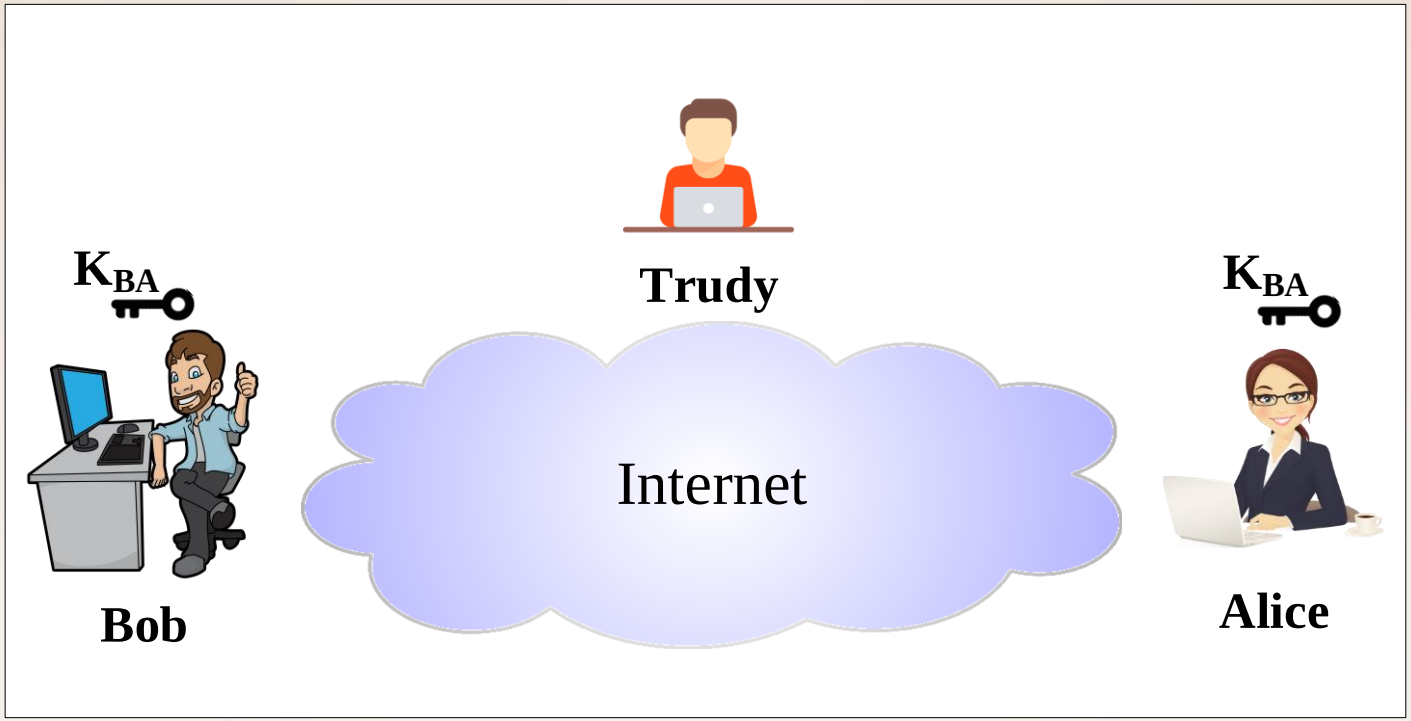
آیا می توان بین دو طرف کاملا غریبه، و از طریق شبکهٔ ناامن و زیر چشم نفوذگران، یک کلید محرمانه و سری سِت کرد؟

nastooh@aut.ac.ir

پروتکل Diffie-Hellman

نیاز اصلی الگوریتم های رمزنگاری متقارن:

کلید مشترک و سری

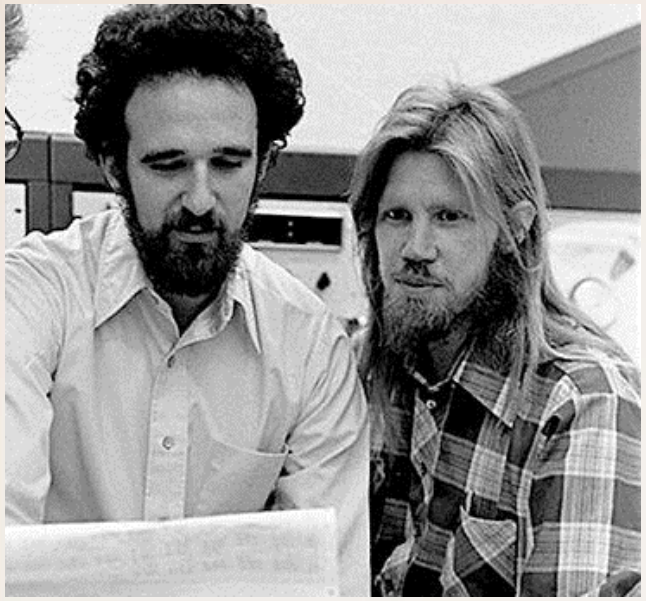


شکل برای توضیح شفاهی

nastooh@aut.ac.ir

پروتکل Diffie-Hellman

- الگوریتم دیفی-هِلمن
  - هدف: سِت کردن یک کلید مشترک و سری، بین دو طرفِ کاملا غریبه، از طریق شبکهٔ ناامن.



مرجع

Cryptography and Network Security, William Stallings, 7th ed.,
Section 10.1.

پروتکل Diffie-Hellman

- الگوریتم دیفی-هِلمن
  - هدف: سِت کردن یک کلید مشترک و سری، بین دو طرفِ کاملا غریبه، از طریق شبکهٔ ناامن.

  - فرضیات:
    - باب و آلیس نیاز به یک کلید مشترک و سری دارند.
    - شبکهٔ ارتباطی آنان به طور کامل توسط ترودی شنود می شود... کامل!
    - ترودی همهٔ الگوریتم ها، حتی دیفی-هلمن را به طور کامل می داند.

nastooh@aut.ac.ir

پروتکل Diffie-Hellman

- الگوریتم دیفی-هِلمن
  - مرحلهٔ اول: **توافق** آلیس و باب بر روی دو عدد با نام n و g:
    - n باید اول باشد،
    - g باید یکی از مولدهای میدان Z_n باشد. (یادآوری در اسلاید بعد)
    - انتخاب n و g با جستجو و تست صورت میگیرد.
    - وجود g برای n، لزوما یکتا نیست.

- این دو عدد سری و محرمانه نیستند. مثلا می توانند توسط یکی از طرفین به دیگری پیشنهاد شوند. که قاعدتاً ترودی نیز مطلع می شود!

nastooh@aut.ac.ir

پروتکل Diffie-Hellman

✓ الگوریتم دیفی-هِلمن

یادآوری:

اگر n اول باشد، فرض کنید به ازای عدد a، مجموعهٔ $<a>_n$ را به صورت زیر تعریف کنیم: تمام باقیمانده های ممکن تقسیم توانهای مختلف a بر n

- مثلا: اگر n=7 باشد، به ازای a=2 توانهای مختلف عدد ۲، به پیمانهٔ ۷ فقط و فقط اعداد ۱ و ۲ و ۴ خواهند شد.

اما به ازای a=3، توانهای مختلف عدد ۳، به پیمانهٔ ۷، می تواند اعداد ۱ و ۲ و ۳ و ۴ و ۵ و ۶ باشند. پس با نوتیشن بالا می گوییم:

$<2>_7=\{1, 2, 4\}$ $<3>_7= \{1, 2, 3, 4, 5, 6\}$

- حال به زبان ساده g را یک مولد برای Z_n گوییم، اگر

$$<g>_n=\{1, 2, 3, \ldots., n-1\}$$

nastooh@aut.ac.ir

پروتکل Diffie-Hellman

- ✓ الگوریتم دیفی-هِلمن
  - مرحلهٔ دوم: باب و آلیس باید هر کدام یک عدد جدید انتخاب کرده و نزد خود **محرمانه** نگهدارند.

- فرض می کنیم باب عدد x و آلیس عدد y را انتخاب کرده اند.
- نیازی به تبادل این اعداد نیست.
- هرچه اعداد بزرگتر باشند، بهتر است. (مثلا ۵۱۲ بیتی)
- ترودی از این اعداد مطلع نیست، زیرا محرمانه هستند و بر روی شبکه ارسال نمی شوند.

پروتکل Diffie-Hellman

- ✓ الگوریتم دیفی-هِلمن
  - مرحلهٔ سوم: باب مقدار $g^x \mod n$ را محاسبه کرده و برای آلیس ارسال می کند.
    - قاعدتاً این مقدار به دست ترودی هم خواهد رسید.
  - مرحلهٔ چهارم: آلیس متقابلاً مقدار $g^y \mod n$ را محاسبه کرده و برای باب ارسال می کند.
    - قاعدتاً این مقدار به دست ترودی هم خواهد رسید.

nastooh@aut.ac.ir

پروتکل Diffie-Hellman

- الگوریتم دیفی-هِلمن
  - مرحلهٔ پنجم: باب مقدار دریافتی از آلیس را به توان x رسانده و باقیماندهٔ آن بر n را محاسبه می کند. یعنی مقدار: $(g^y \bmod n)^x \bmod n$
  - مرحلهٔ ششم: آلیس متقابلاً مقدار $(g^x \bmod n)^y \bmod n$ را محاسبه کرده می کند.

طبق نظریه اعداد (لگاریتم گسسته)، حاصل محاسبات مرحلهٔ پنج و شش، یکسان است:

$$g^{y.x} \bmod n$$

این همان کلید مشترک و سری خواهد بود

nastooh@aut.ac.ir

پروتکل Diffie-Hellman

- ابتدا یک مثال از دیفی-هلمن
  - انتخاب n=23 و g=5 به طور مشترک.
    - بر اساس روال مطرح شده، برا g انتخابهای دیگری نیز داریم، مانند: ۷ یا ۱۰ یا ۱۱.
  - انتخاب x=15 توسط باب و y=6 توسط آلیس.
  - ارسال ۱۹ توسط باب برای آلیس. ($5^{15} \bmod 23 = 19$)
  - ارسال ۸ توسط آلیس برای باب. ($5^{6} \bmod 23 = 8$)
  - محاسبهٔ کلید برابر ۲ توسط باب. ($8^{15} \bmod 23 = 2$)
  - محاسبهٔ کلید برابر ۲ توسط آلیس. ($19^{6} \bmod 23 = 2$)

هر دو به کلید مشترک ۲ رسیدند.

سوال مهم

پس ترودی چه؟

nastooh@aut.ac.ir

پروتکل Diffie-Hellman

- ✓ بررسی وضعیت مهاجم در پروتکل دیفی-هلمن
  - داشته های ترودی:
    - n (در مثال قبل ۴۷)
    - g (در مثال قبل ۳)
    - مقدار عبارت $g^x \mod n$ (در مثال قبل ۲۸)
    - مقدار عبارت $g^y \mod n$ (در مثال قبل ۱۷)
  - نداشته های ترودی:
    - فقط x و y
  - ترودی اگر x را داشته باشد، میتواند مثلا ۲۸ را به توان x رسانده و باقیماندهٔ آن بر n را محاسبه کند و به کلید دست یابد.
  - از طرفی این معادلهٔ را دارد: $3^x \mod 47 = 28$، در ظاهر معادله ای ساده با سه معلوم و یک مجهول!!!
    - تنها راه: جستجوی کامل... زمان؟؟ رجوع به مبحث لگاریتم گسسته.

nastooh@aut.ac.ir

پروتکل Diffie-Hellman

- ✓ یک مشکل خاص

Man In The Middle!

- ترودی، هنگام سِت کردن کلید بین باب و آلیس، می تواند حملهٔ مرد میانی را بر علیهٔ پروتکل زیبای دیفی-هلمن پیاده کند. ☹

- سوال مهم: فرض کنید در میانهٔ پروتکل، باب یک عدد را از آلیس به عنوان پاسخ محاسبهٔ $g^y \bmod n$ دریافت کند. باب از کجا بداند این عدد واقعا از جانب آلیس آمده است؟
  - با توجه به جایگاه اجراییِ این پروتکل –قبل از ست کردن کلید و بالتبع قبل از هیچ گونه روال احراز هویتی- این مساله را در نظر بگیرید.

nastooh@aut.ac.ir

پروتکل Diffie-Hellman

Man In The Middle!

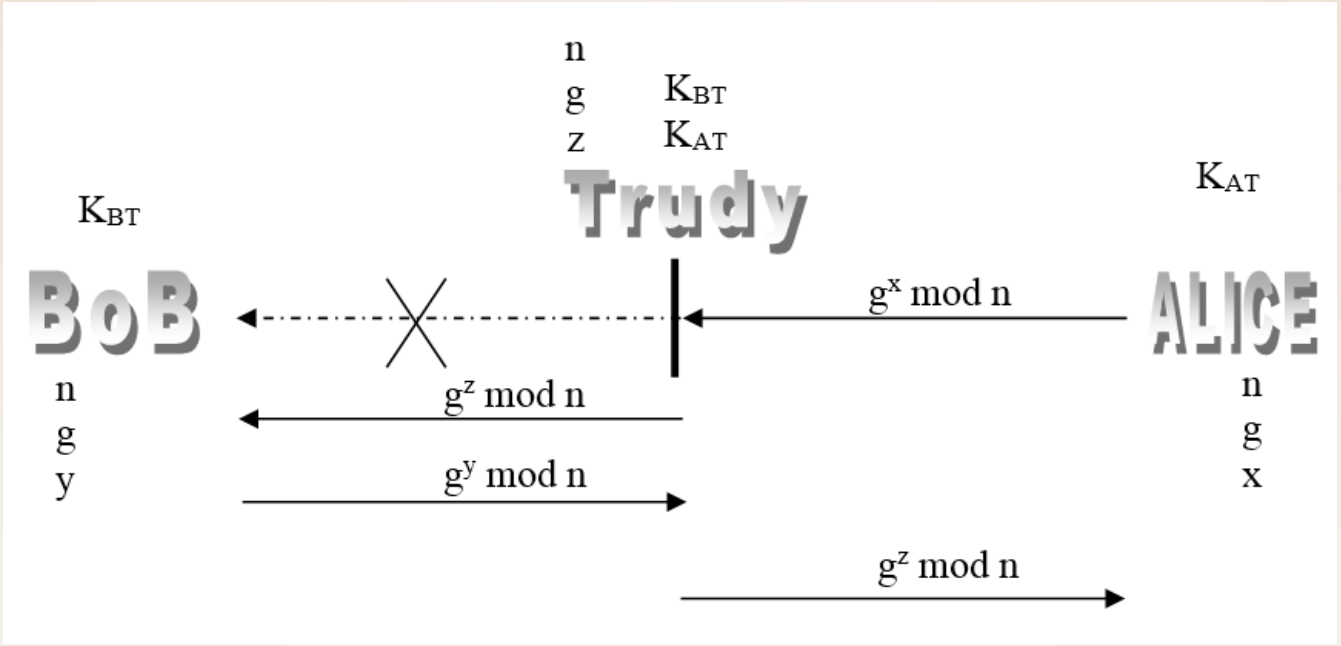
- سناریوی زیر را در نظر بگیرید:
- آلیس پیامی را برای باب ارسال می کند، اما در بین راه توسط ترودی متوقف می شود. و تروی به جای آن عدد $g^z \mod n$ را برای باب ارسال می کند.
  - که z عدد انتخابی ترودی است!
- در پاسخ، باب نیز عدد خود را ارسال می کند، که ترودی بین راه آن را نیز متوقف کرده و همان $g^z \mod n$ را برای آلیس ارسال می کند.
- حال هر سه محاسبات خود را انجام می دهند.
- نتیجهٔ حاصله:
  - باب یک کلید با ترودی ست کرده است. بر اساس x و z
  - آلیس نیز یک کلید با ترودی ست کرده است. بر اساس y و z

nastooh@aut.ac.ir

پروتکل Diffie-Hellman

Man In The Middle!

- سناریوی زیر را در نظر بگیرید:



- ترودی کلید K_{BT} را با باب و کلید K_{BA} را با آلیس ست می کند.
  - اما باب و آلیس گمان می کنند با یکدیگر کلید مشترک ست کرده اند!

nastooh@aut.ac.ir

منابع

[1] William Stallings, “Cryptography and Network Security,” 7th ed.

nastooh@aut.ac.ir

پایان

nastooh@aut.ac.ir