ریاست جمهوری

سازمان مدیریت و برنامه ریزی

مرکز آموزش و پژوهش

امنیت کاربری فناوری اطلاعات (اکفا)

مدرس: مهدی هدایت فر

جلسه اول

مفاهیم امنیت سایبری

جلسه دوم

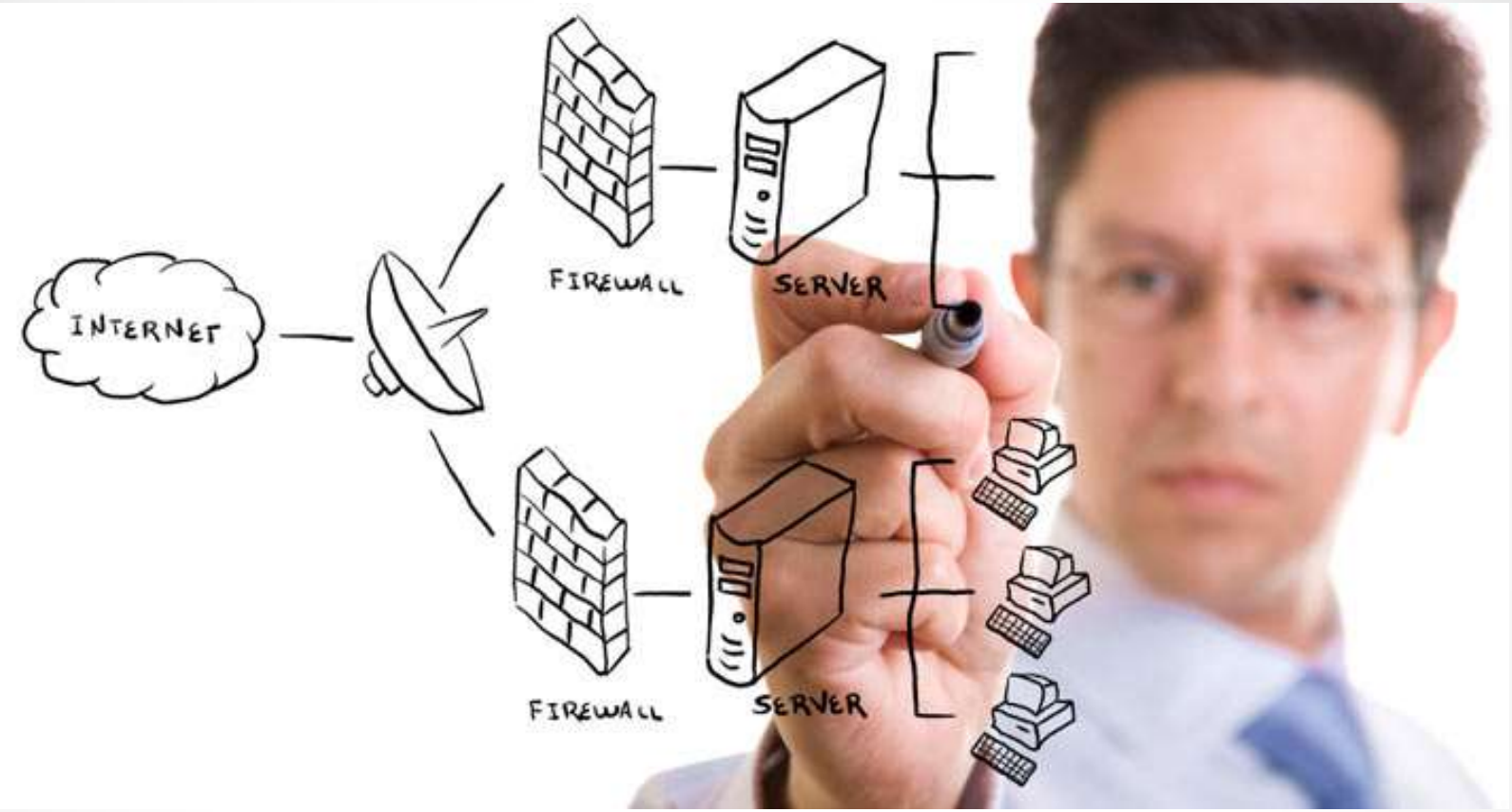
بهداشت سایبری و مفاهیم حقوقی

جلسه سوم

روشهای کنترل و مقابله

جلسه چهارم

نهادهای متولی و کار عملی



روشهای مقابله

قیاس یک شبک Lan با یک قلعه ویا شهر

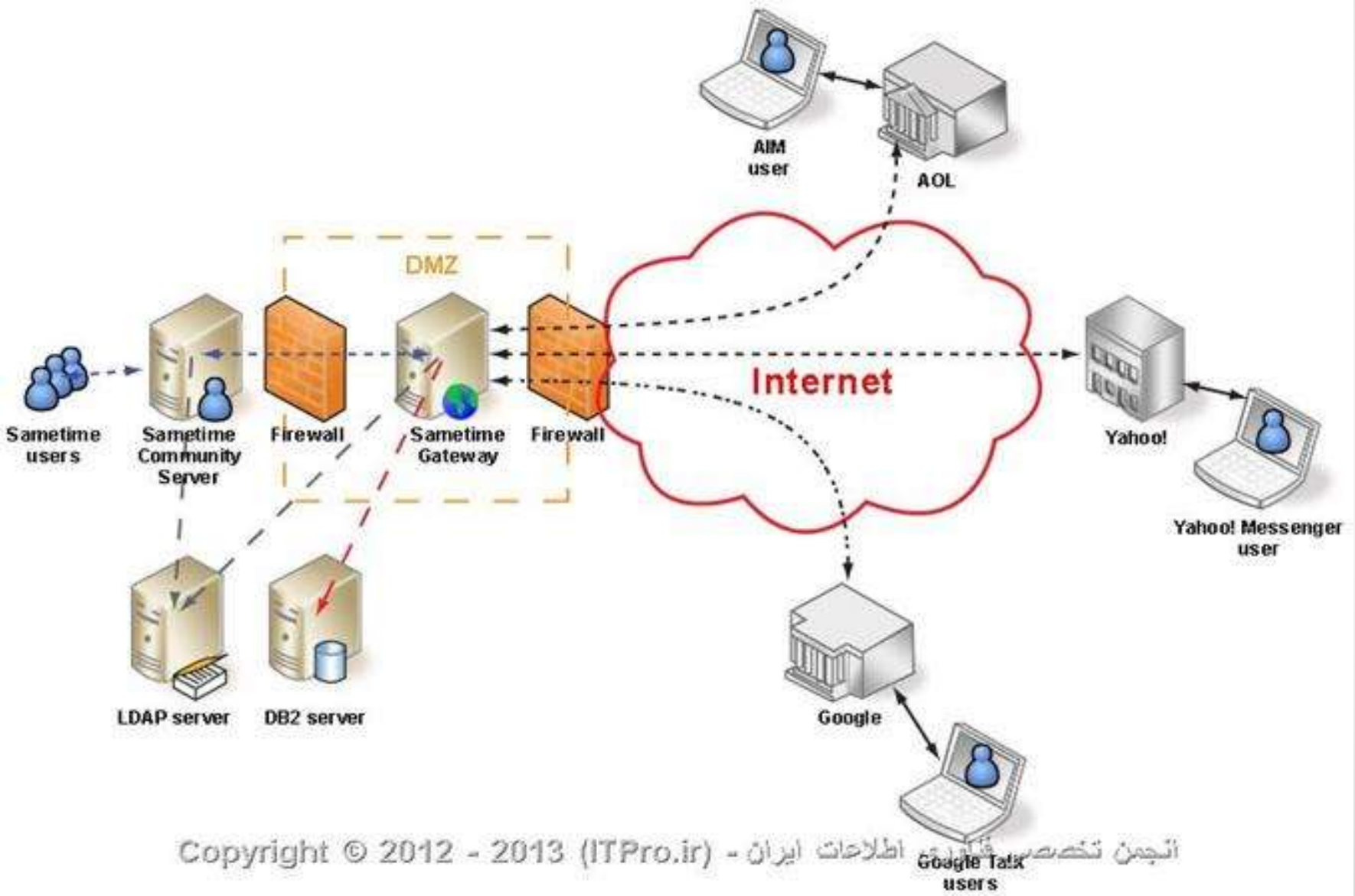
دیوارها: دیواره آتش (Firewalls)

پل ها: کانالهای ارتباطی (VPN یا Tunnels)

خندق ها : منطقه دفاعی مقدم (DMZs)

یک شبکه است که در میان شبکه خصوصی یا داخلی شما و شبکه خارجی یا اینترنت قرار DMZ می گیرد . این شبکه به کاربران خارج از سازمان اجازه برقراری ارتباط با سرورهای داخلی سازمان بصورت مستقیم را نمی دهند و به همین وسیله از اطلاعات سازمان حفاظت می کند. یک لایه امنیتی اضافی برای شبکه را فراهم می کند، زیرا هکرها توانایی DMZ شبکه دسترسی مستقیم به سرورهای داخلی و داده ها از طریق اینترنت را محدود می کنند.

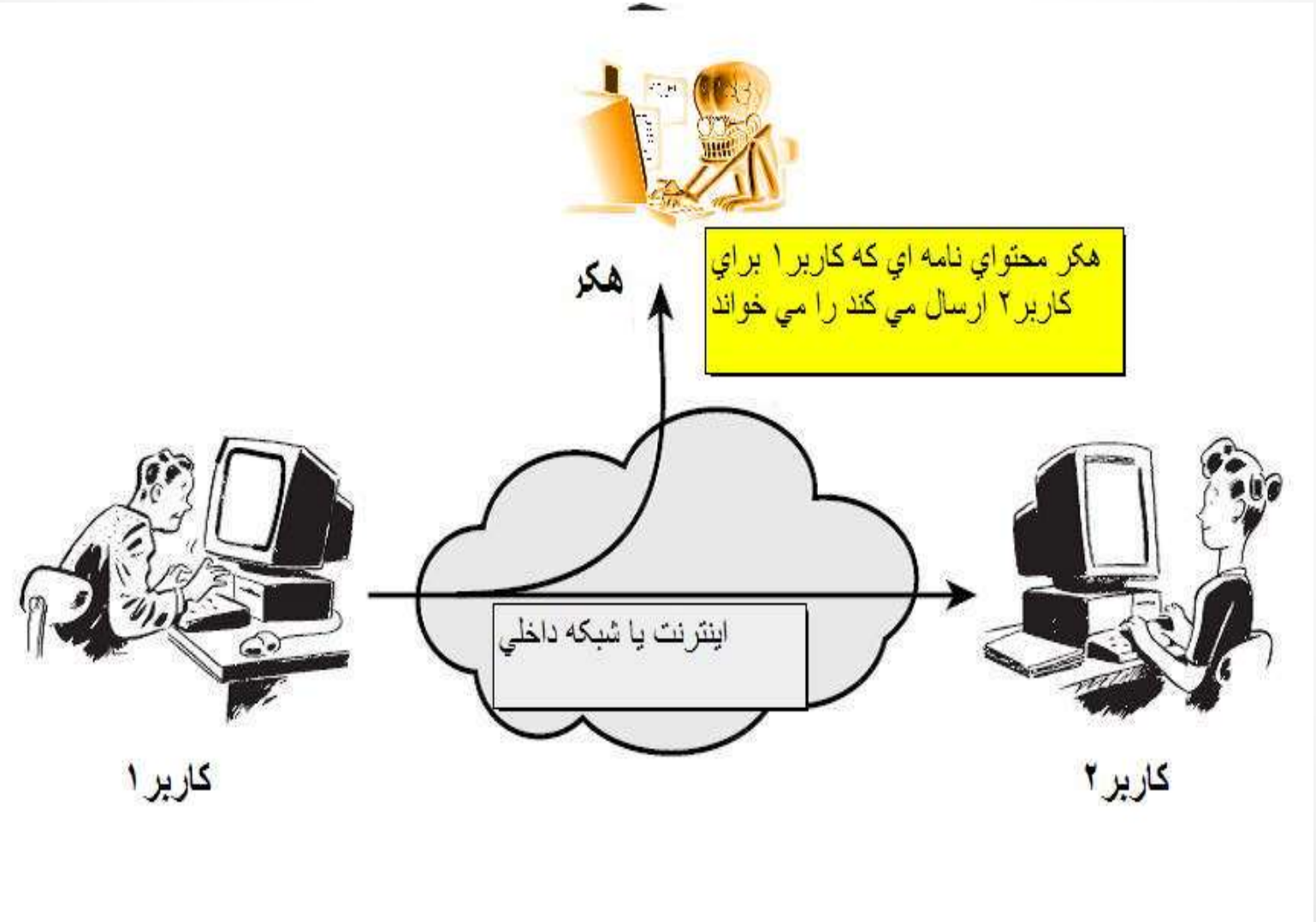
توپولوژی امنیتی



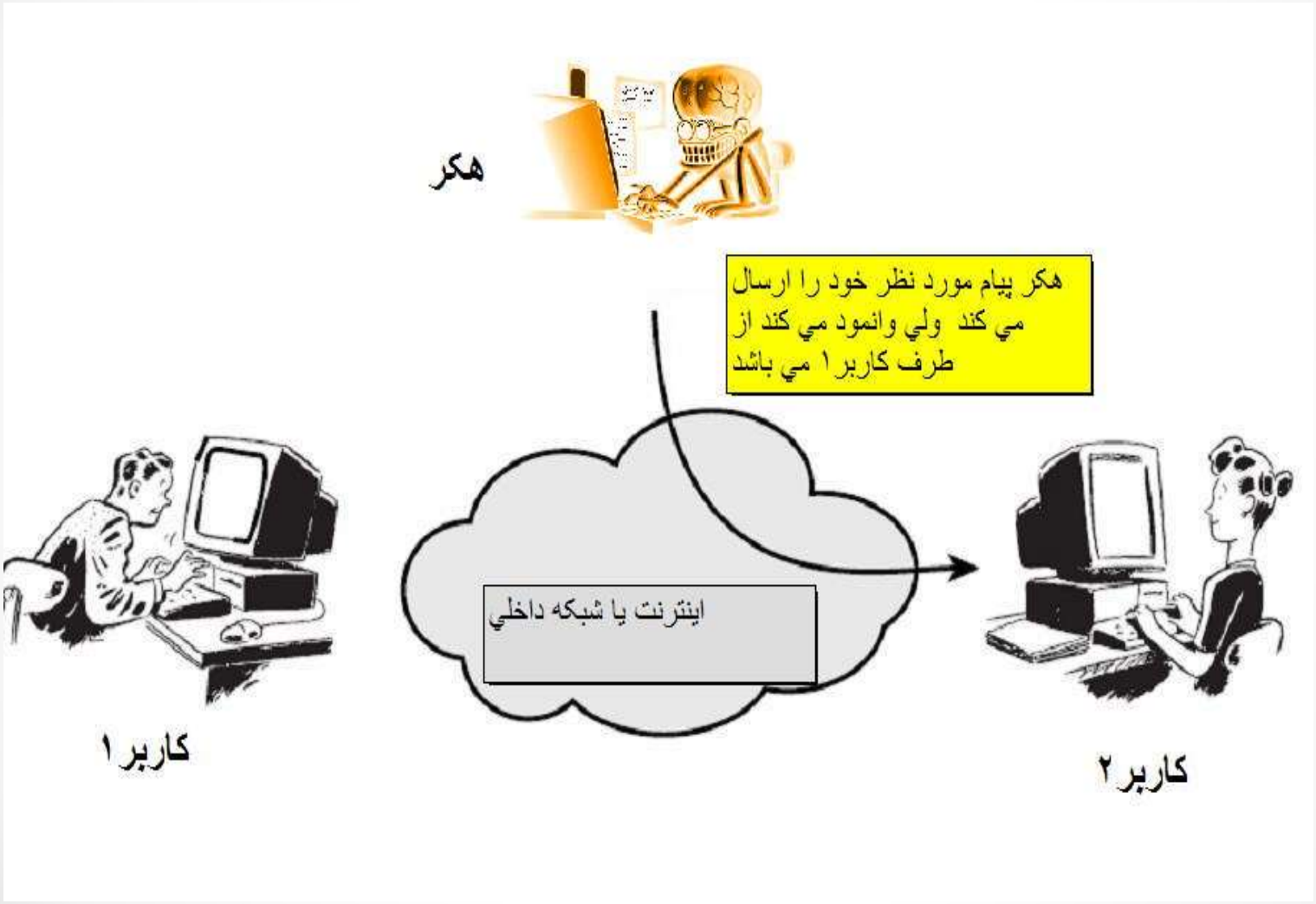
اما نبرد تروآ نشان داد این اقدامات کافی نیست

چند نمونه مشابه از نفوذ هکرها به شبکه ها

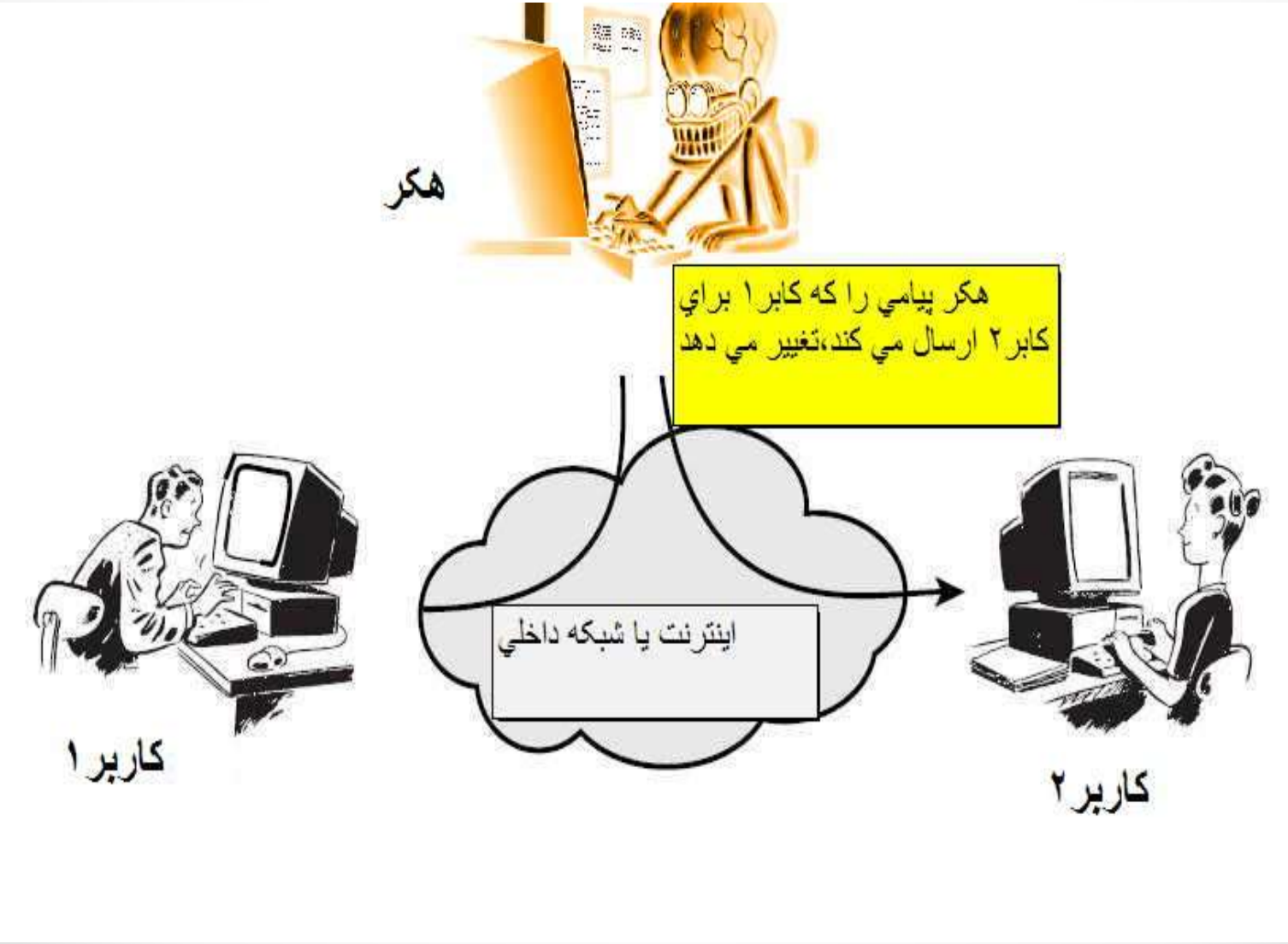
چند نمونه مشابه از نفوذ هکرها به شبکه ها

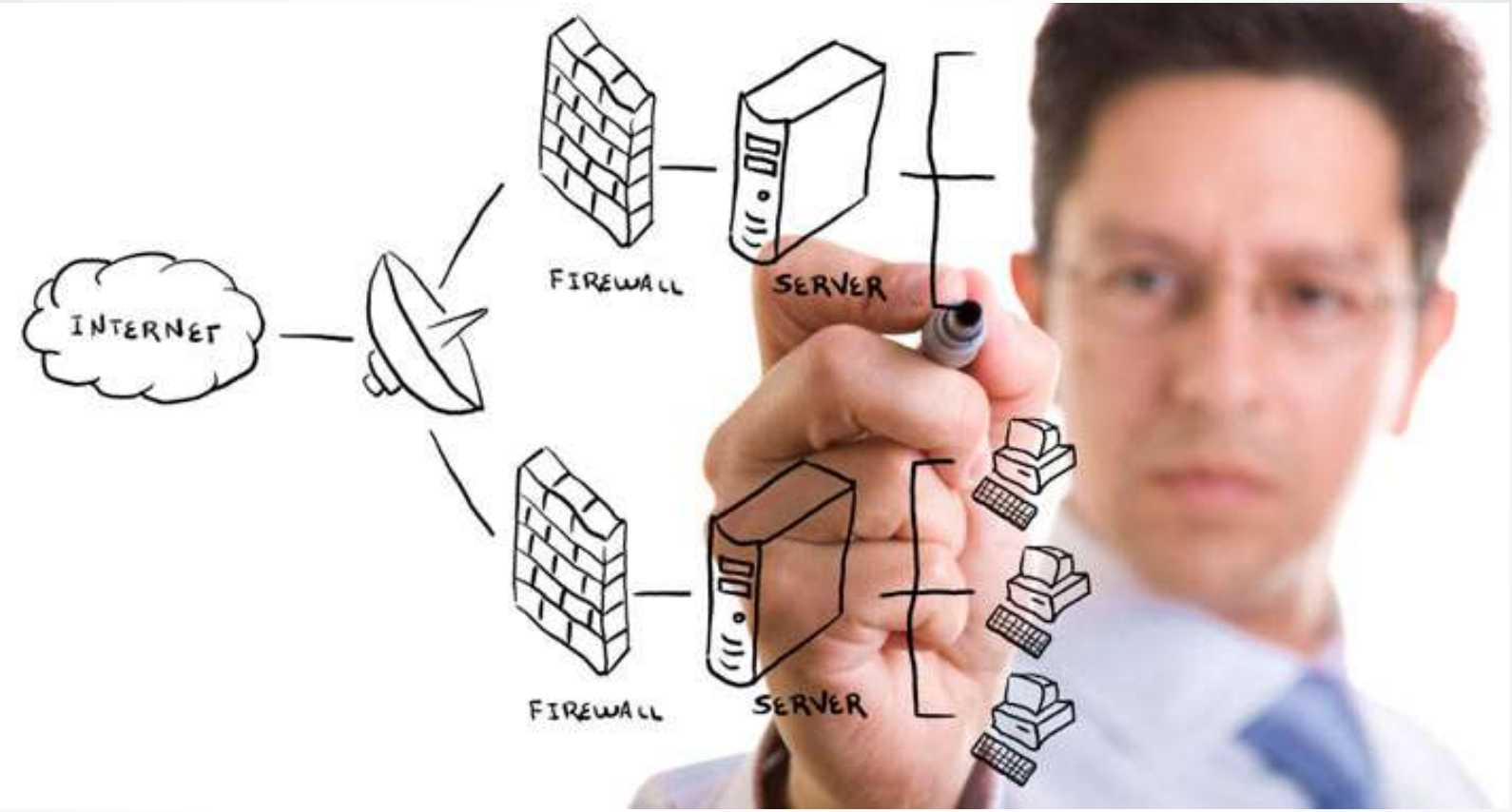


چند نمونه مشابه از نفوذ هکرها به شبکه ها



چند نمونه مشابه از نفوذ هکرها به شبکه ها

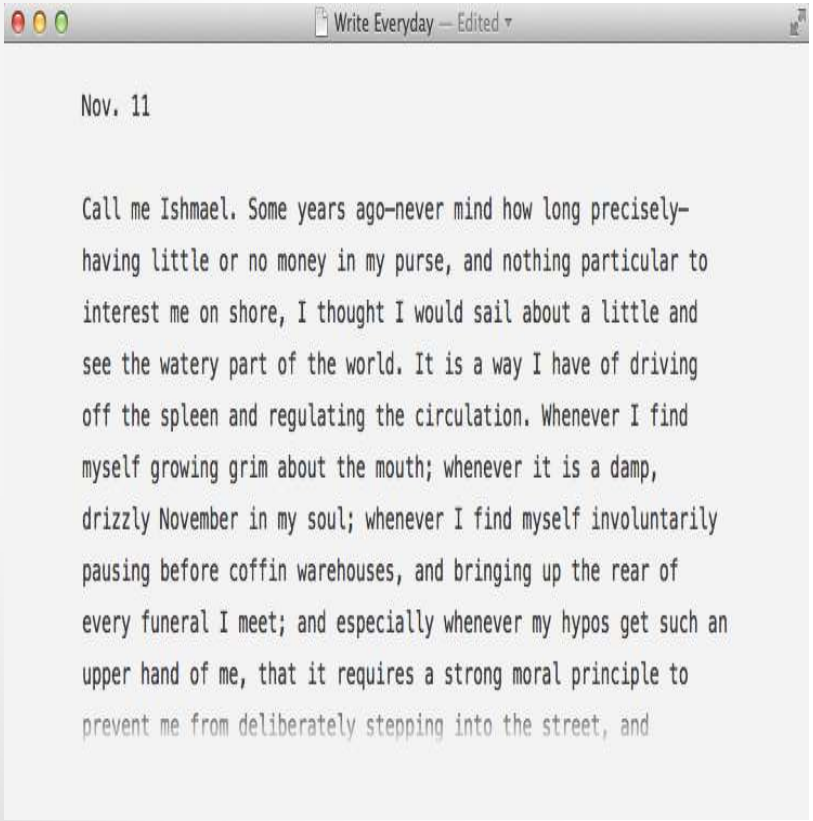




رمزنگاری

چند تعریف در رمزنگاری

متن آشکارPlaintext

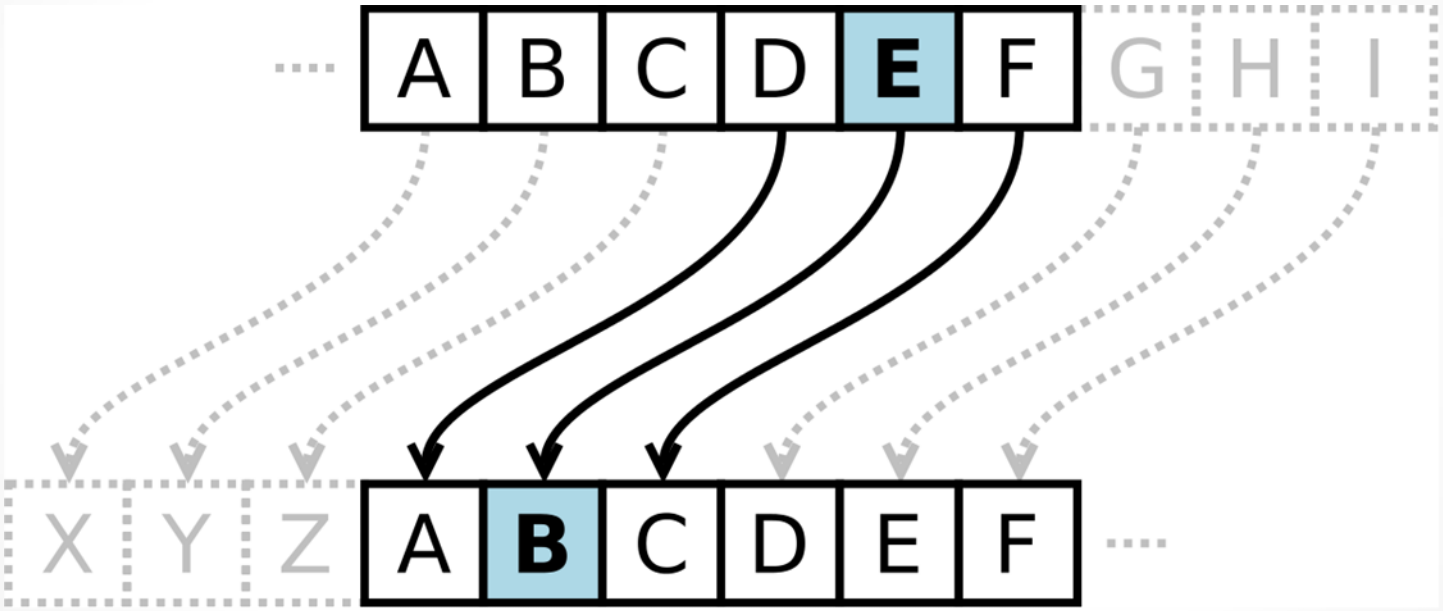


متن رمز Ciphertext

```
hQIMAw3Jn/nLK/38ARAAsSXLDhCtzUYKMptNxZImJXwhhIRm3QxfuyHjJ93ASylE
e+6ABkuyFLJhiKryxp/JmS/alMPfF7hx2aTgovagaPzTwTV1jo6If2mhdCl6keed
1Iz7C0f6jHIqq9d8g0bWDyvELEipn5LNDTX3Xp2Csx5ojRB2wckrUtl1lXyj8G0H
4DQUYbINRmJVulJJC/acGvgOze66pHuRgSCxxHDscefjXenh/XejSYTo7aMi+Es7
DCcD49zH6ZLDQN6BlN9q2oFI8QIhQ2y1QJbat1dWi/4yYWlKZcLKRSm8eo/gNCdL
h9MncXBBSfgbvbu67CDZ9GO5geZOn3LzQOpJ8hrZq/6K/uMcUKeZjW3RCo0T754f
E5zYe1wUgtwS/lmQ2w5PQF/89bpshtDSYuL1fZgzrsE6DwophuCri5zwCGbEKlsI
g6REIETFbZ2aCL4N2pZVunCIEuoP0zgEB6+M9egdpyxMsMqEBVg3AH7Sa1AtEguP
T/MCxI0bZHCUhPupEKT8slbSrDNxTWMUXQt3XpL0bGCCrDMKLSoWYfDiNnRkFbWK
iiqw9hx4Q9CJg7xX7JRnVgwOeREiFnMYSbFlvPSxEOu6FdBYhdqSefKin4Wnkmdw
qrSl8fjIW/kZ2v72uz0buEKkY9ubBox76yjlRo9KUQMs3em03kc64959gTDiZ0qF
AgwDrosDPQ2BeYQBD/9H5VKFw0an5j5MX1JpOSBAqNGKWq2bcEFnwJfk0DDlhyHD
owHiG7gDowCS+5y/pf56v36HkzpJZATKqoRyKVxmQOxU9l3YnPc5fw8iFhxlrfcG
ywzkJh/BRDQ/uy5fhGc/PbSm6iLv/SkkWTK8PSUD+g1yZyK0W7WkMh9QYS2OE7lQ
qbwpNiy57reWkUWCoE4QmKqqpe7NXXM0eLT9l2D0hG2lthyvTvspkpxszl8+HMJv
M2LMcY2FmmZWAJSdxsQSq9NQdyvCJX2D8oa89WQyXmp7mPXL7BQfoQNPndmn6Obi
0EQojoeMRNh14XNhMjPjxW7m34rH2gtvdN3Dg8iFrtocoVJqXqU3N+9T2sNe/bS8
```

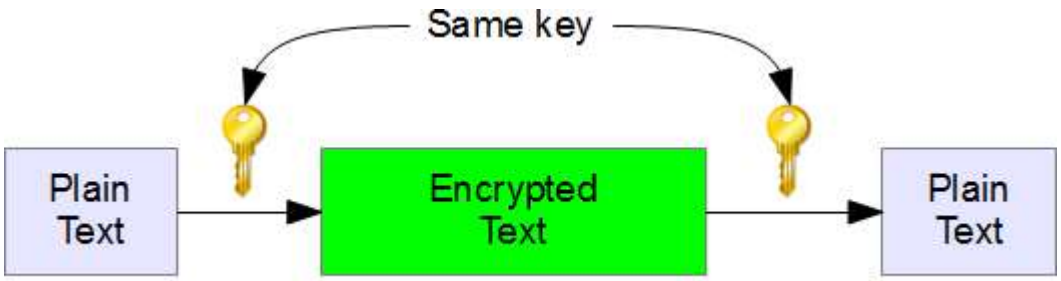
چند تعریف در رمزنگاری

الگوریتم رمزنگاری



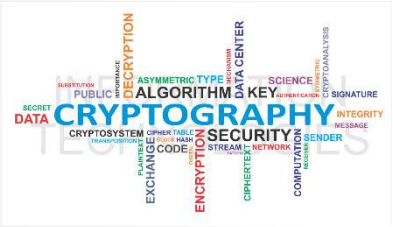
چند تعریف در رمزنگاری

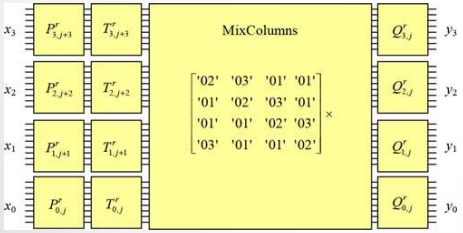
کلید key



اطلاعاتی که در Cipher استفاده میشود و فقط فرستنده و یا گیرنده آن را میدانند

چند تعریف در رمزنگاری





- رمز گذاری(**Encipher,Encrypt**)

  تبدیل Plaintextبه Ciphertext

- رمز گشایی(**Decipher,Decrypt**)

  استخراج Plaintextاز Ciphertext

- رمز نویسی(**Cryptography**)

  علم اصول روش های encryption

- تحلیل رمز(**Cryptanalysis**)

  علم اصول و روش های Decryptionبدون اطلاع از Keyکه به آن به اصطلاح codebreakingهم گفته میشود

- رمز نگاری(**Cryptology**)

  و بالاخره رمز نگاری یعنی علم حاصل از ترکیب Cryptographyو Cryptanalysis

رمزنگاری متقارن-Symmetric

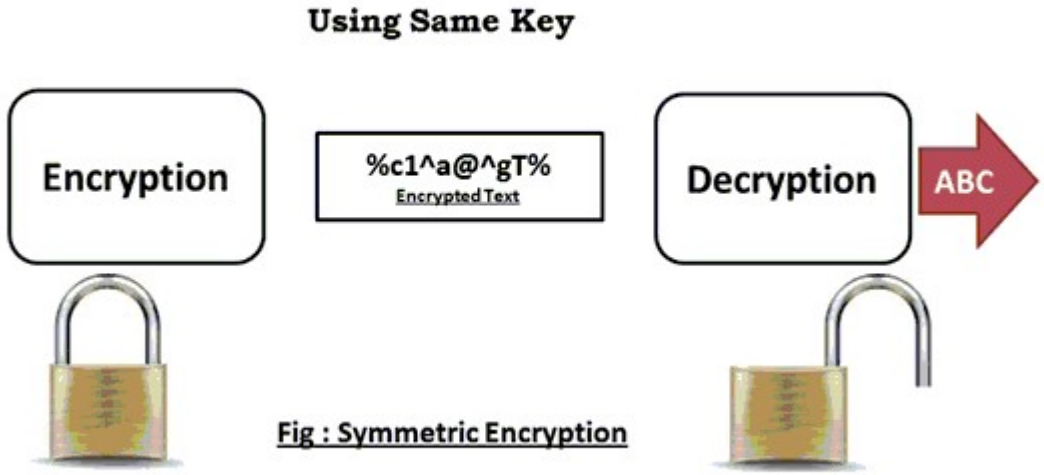


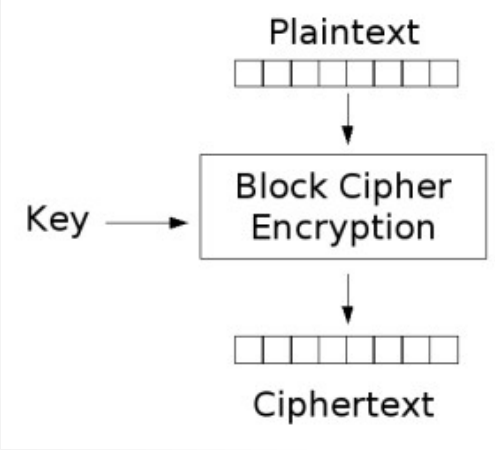
Fig : Symmetric Encryption

در این روش از کلید مشترک برای Encryptو Decryptاستفاده میشود از الگوریتم های معروف آن

- AES
- DES
- 3DES
- Blowfish
- RC4
- ..

رمزنگاری متقارن-Symmetric

مز های متقارن را میتوان به دو روش عمده تولید کرد:



- رمز های قطعه ای(Block Cipher)

در این نوع پردازش پیام های به صورت قطعه ای انجام میشود که اندازه متعارف قطعات ۶۴ و ۱۲۸ یا ۲۵۶ بیت است

الگوریتم های Blowfish,DES,3DES,AESاز این نوع هستند

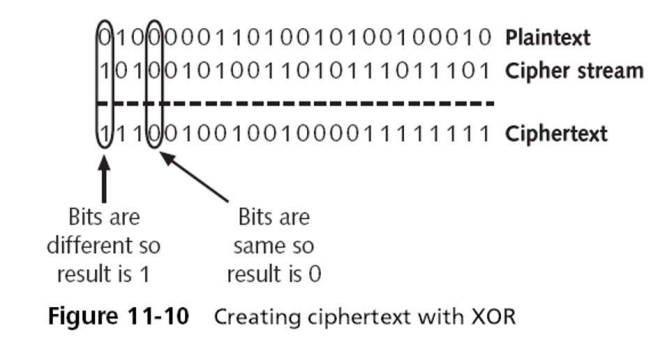


Figure 11-10 Creating ciphertext with XOR

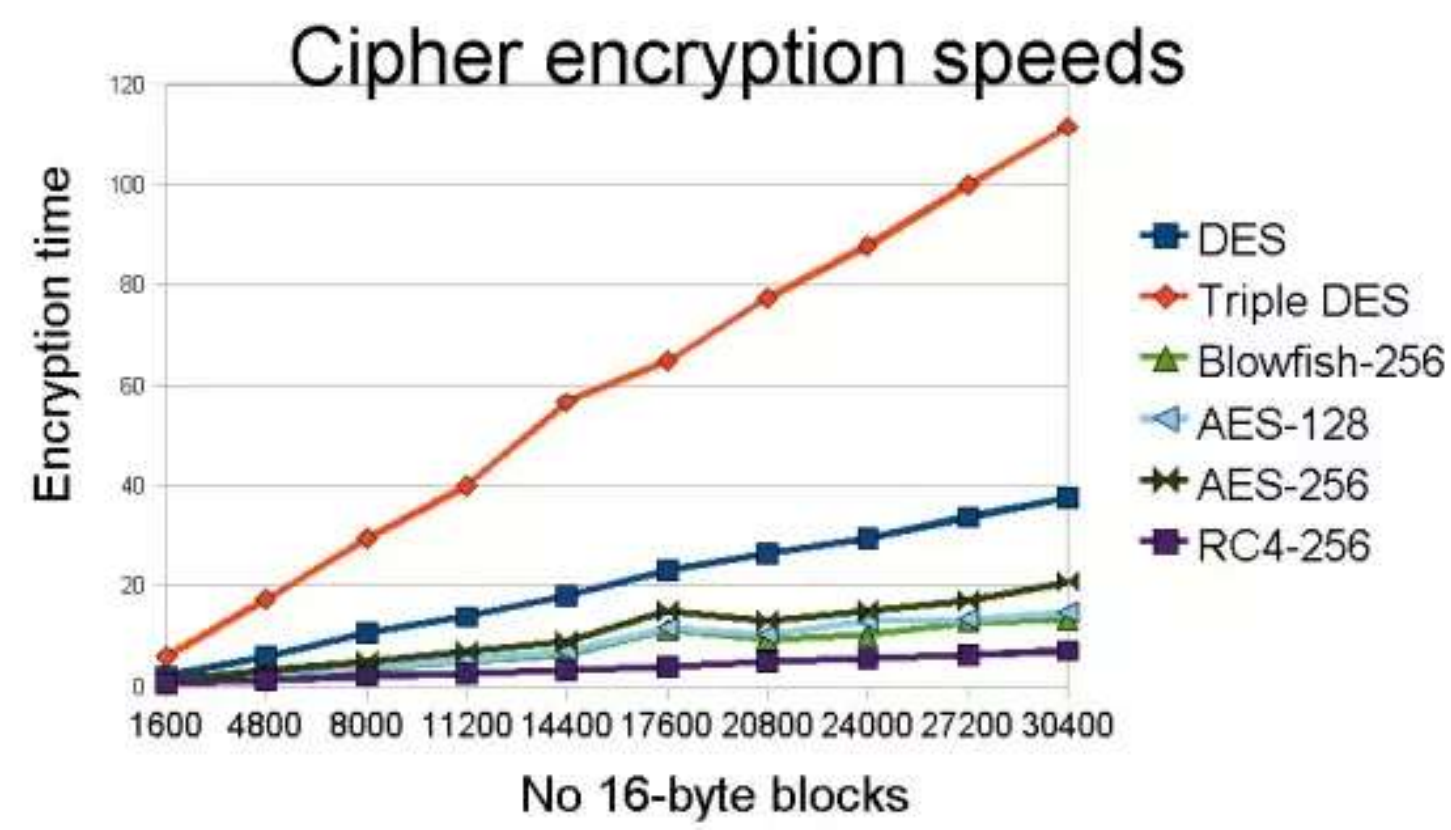
- رمز های جریانی(Stream Cipher)

در این نوع پرداز پیام به صورت پیوسته انجام می شود

الگوریتم RC4از این نوع است

رمزنگاری متقارن-Symmetric

benchmarkسرعت الگوریتم های روش متقارن



رمزنگاری نا متقارن-Asymmetric

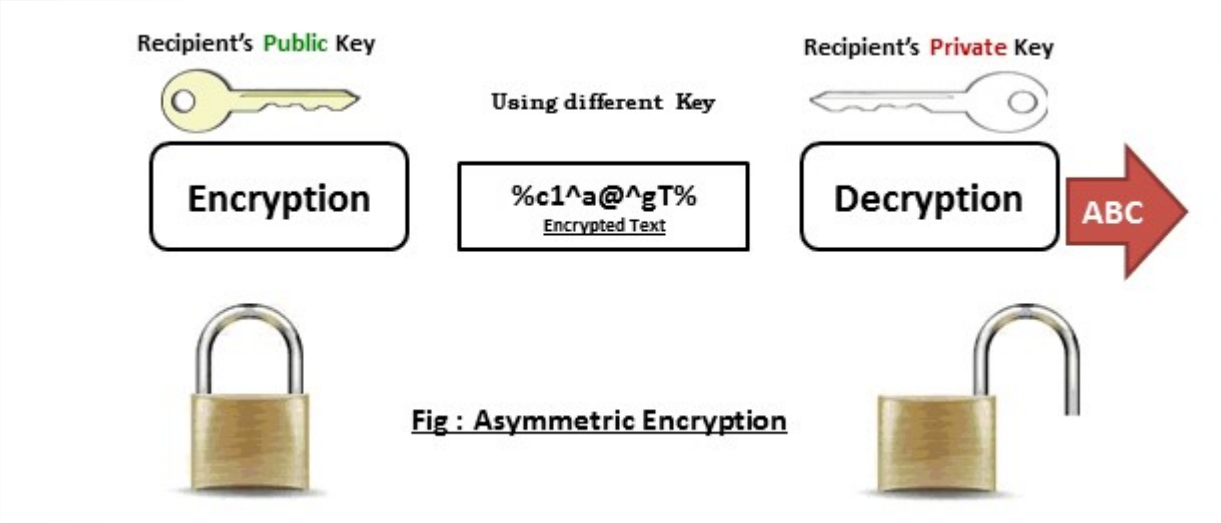


Fig : Asymmetric Encryption

در این روش به جای استفاده از یک کلید مشترک از یک جفت کلید به نام های عمومی(public)و خصوصی(private)استفاده میشود به این صورت که با public key اطلاعات encryptشده و با private key اطلاعات decryptمیشودز الگوریتم های معروف این روش:

RSA

ElGamal

...

رمزنگاری نا متقارن-Asymmetric

RSA (Rivest–Shamir–Adleman)

رمزنگاری نا متقارن-Asymmetric

رمز نگاری نا متقارن برای جایگزینی روش رمز نگاری متقارن به وجود نیامده است بلکه برای تکمیل روش رمز نگاری متقارن به وجود آمده است که به آن اصطلاح کلید عمومی گفته میشود و برای رسیدن به دو هدف طراحی شده است

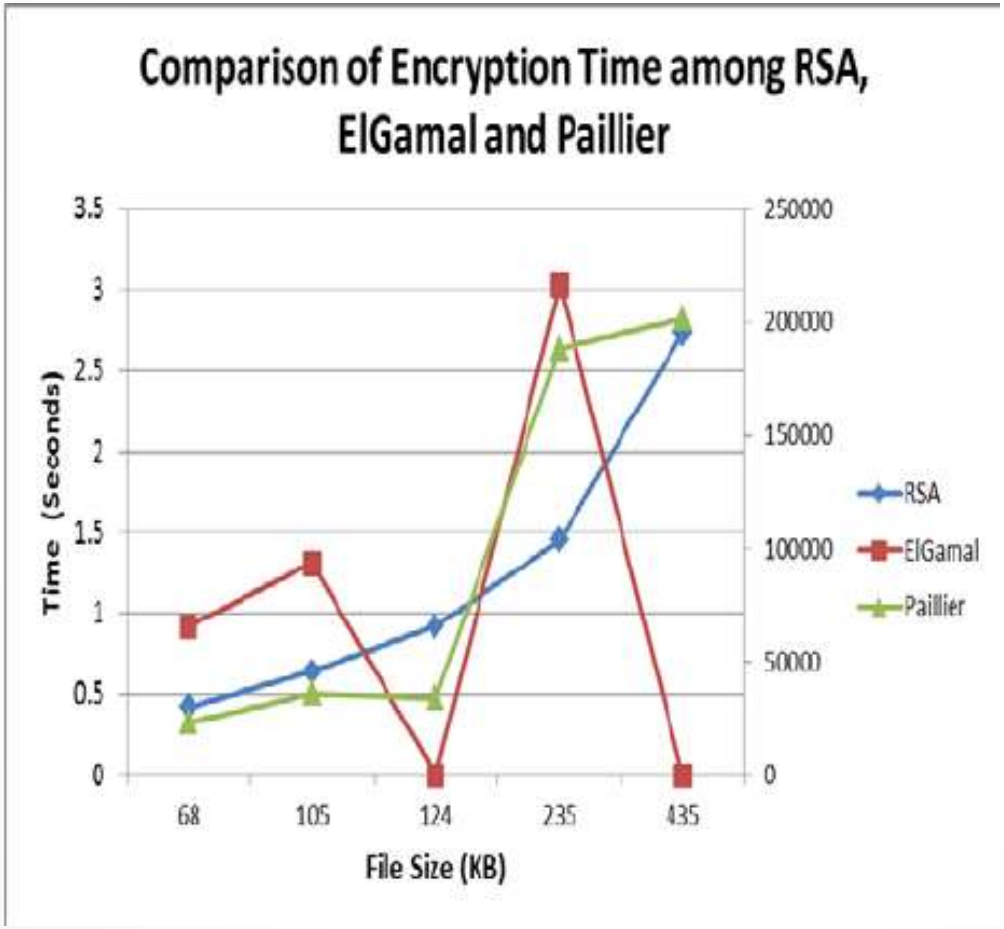
- حل مساله در اختیار داشتن کلید در روش رمز نگاری متقارن
- امضای دیجیتال

ویژگی های روش نامتقارن را میتوان موارد زیر عنوان کرد

- رسیدن به encryption key از decryption key از لحاظ محاسبانی نا ممکن است
- در حفظ محرمانگی(Confidentiality)رمزگذاری امری همگانی است و نیازی به اشتراک گذاری اطلاعات محرمانه وجود ندارد
- در حفظ محرمانگی(Confidentiality)رمزگذاری امری اختصاصی بوده است و محرمانگی پیام ها محفوظ می ماند

رمزنگاری نا متقارن-Asymmetric

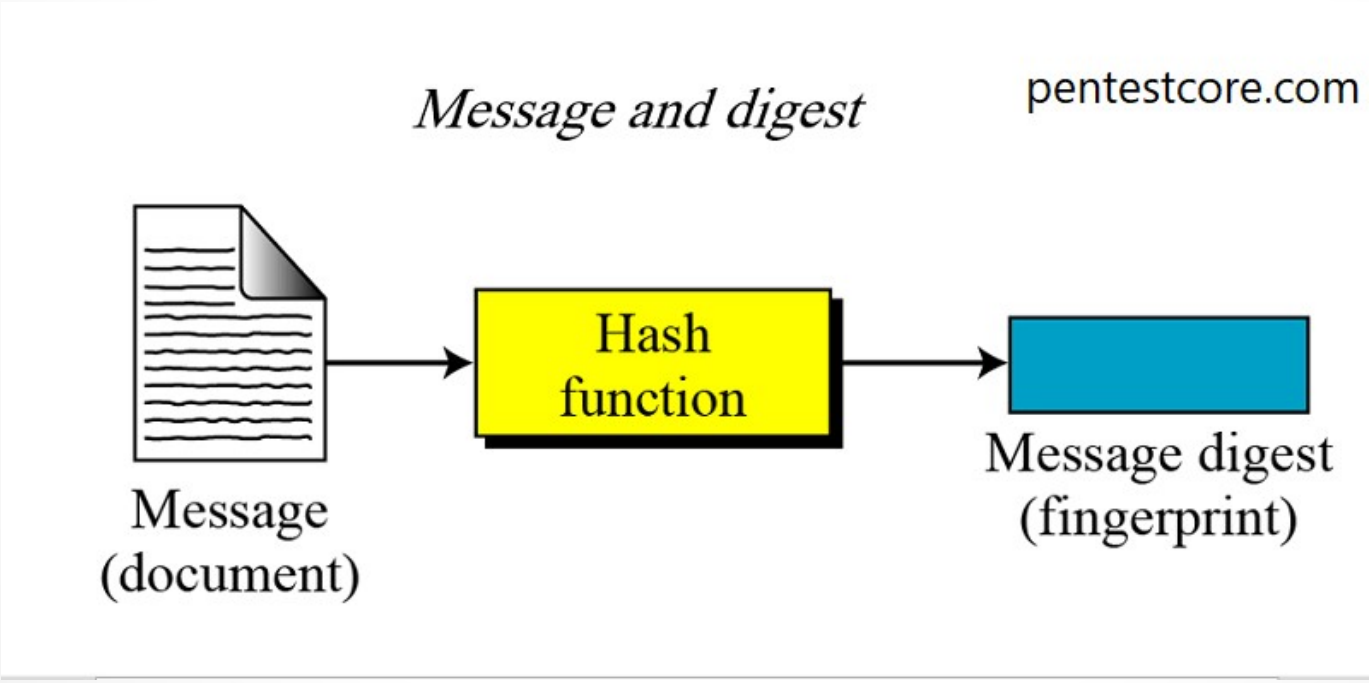
benchmarkسرعت الگوریتم های روش نا متقارن



اگر خواستید الگوریتم RSAرا امتحان کنید به اینجا مراجعه کنید البته که قرار شد private keyمحرمانه باشد! ولی خب برای امتحان بد نیست

هش -hash

الگوریتم هش اطلاعات را در هر اندازه ای(عدد، حروف، فایل های رسانه ای) دریافت کرده و آنها را به یک رشته از اعداد و حروف ثابت تبدیل می کند. این اندازه بیت ثابت می تواند متفاوت باشد(مثل ۶۴ بیت یا ۱۲۸ بیت یا ۲۵۶ بیت). این اندازه بستگی به تابع هش مورد استفاده دارد.



هش -hash

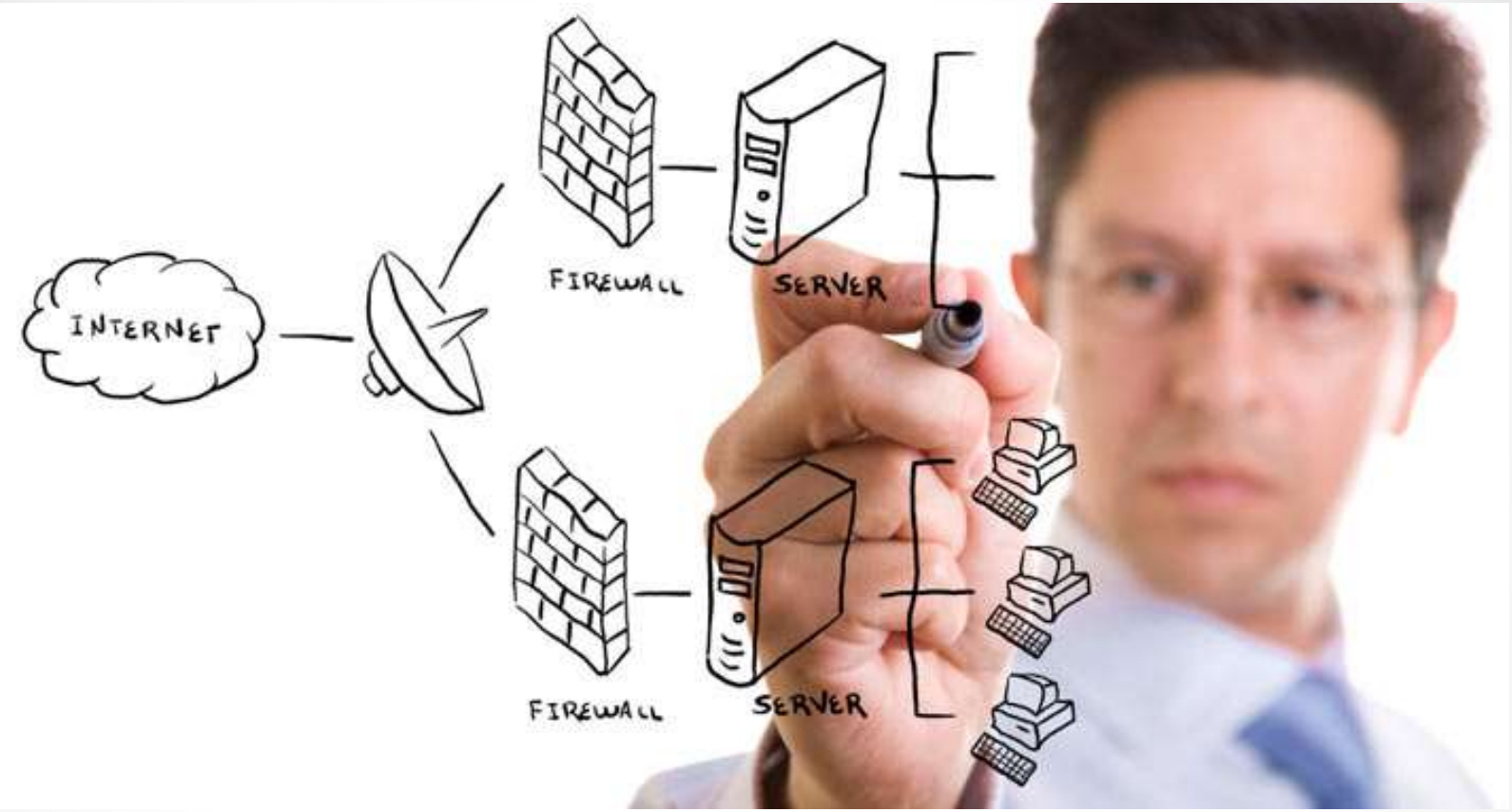
ویژگی ها:

- قطعی بودن
- محاسبه سریع
- غیر قابل بازگشت بودن

INPUT	HASH
Hi	639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

- تغییر کوچک در ورودی، هش را تغییر می دهد

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C



نکات مهم در امنیت سایبری

شیوه‌ها و سیاست‌های امنیت اطلاعات برای کارکنان سازمان

آموزش‌های پرسنل و نکات فنی امنیتی می‌تواند بروز مشکلات امنیتی را کاهش دهد اما وجود سیاست‌ها و رویه‌های کارا برای کارکنان نیز ضروری است؛ زیرا برای کارکنان به وضوح مشخص می‌کند چه چیزی صحیح و قابل قبول و چه چیزی نادرست است.

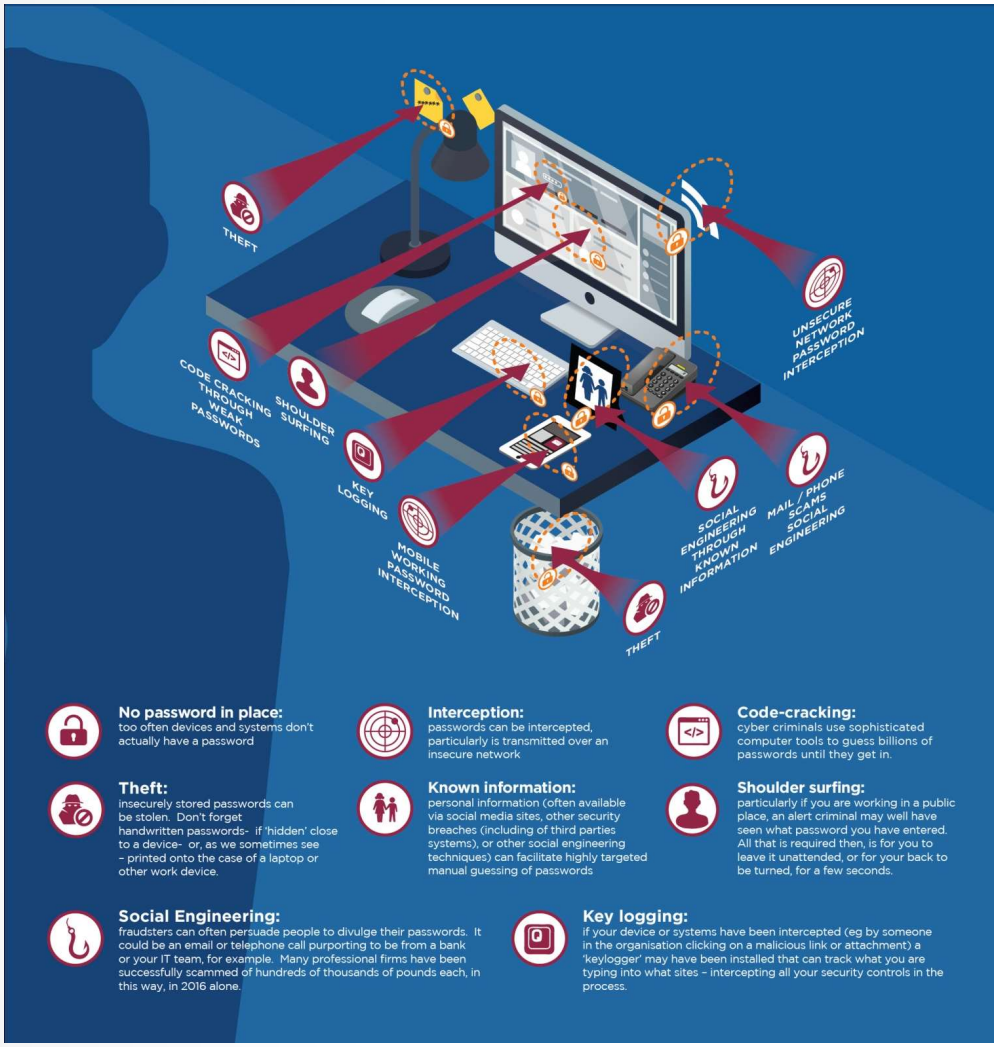
امنیت اطلاعات برای کارکنان سازمان

- ✓ استفاده از کلمات عبــور قــوی و حفاظــت ازآن ها؛
- ✓ قوانین مربوط به دسترسی ایمن از راه دور به شبکه شرکت(ریموت به شبکه شرکت)؛
- ✓ دانلود کردن برای استفاده شخصی (با توجه به بحث هزینه و پهنای باند)؛
- ✓ عدم ارسال مطالب محرمانه یا ایمیل. ارسال مطالب حساس و مهم باید به‌صورت رمزنگاری‌شده باشد؛
- ✓ سهواً یا عمداً دانلود کردن نرم‌افزارهای مخرب؛
- ✓ نشت دسترسی غیرمجاز به اطلاعات مهم و حساس؛
- ✓ استفاده ایمن و مسئولانه از ایمیل؛
- ✓ حفظ اطلاعات محرمانه سازمان؛
- ✓ دسترسی غیرمجاز به اطلاعات مهم و حساس؛

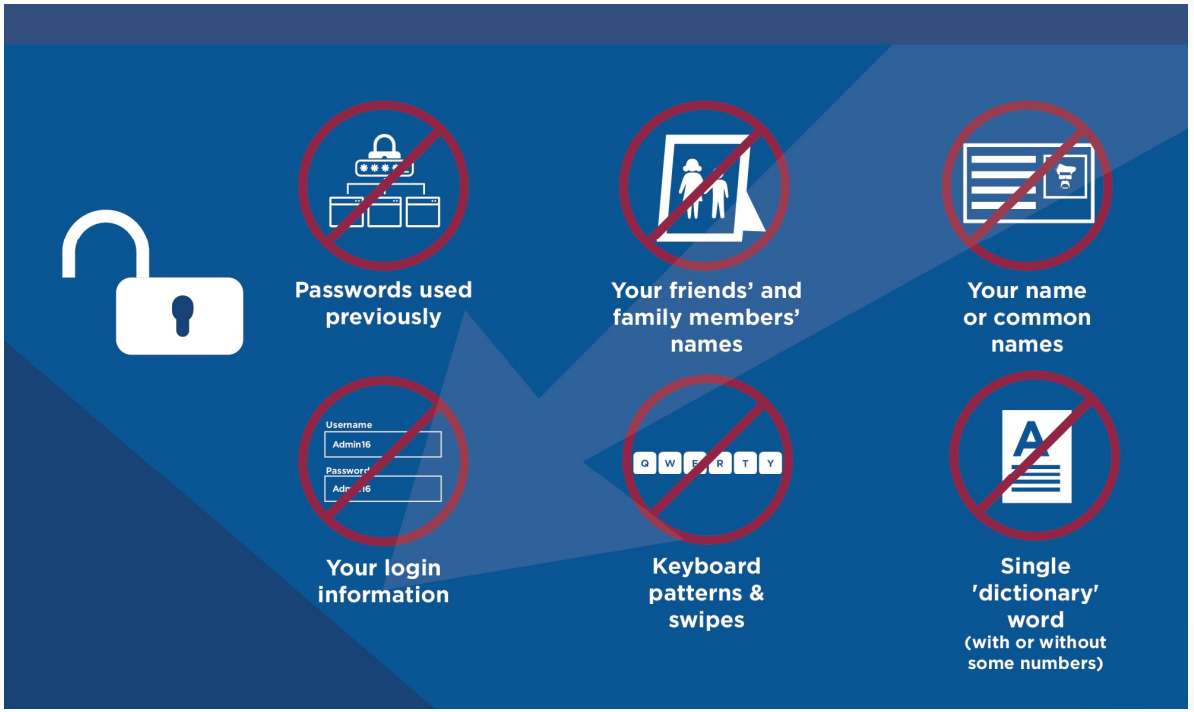
نکات مهم در امنیت سایبری برای شرکت‌ها

- ✓ دانستن اصول امنیتی
- ✓ محافظت از اطلاعات، کامپیوترها و شبکه‌ها
- ✓ عدم استفاده شخصی از اینترنت و پهنای باند
- ✓ اتصال به اینترنت فقط از طریق فایروال
- ✓ اعمال سیاست دستگاههای قابل حمل
- ✓ پشتیبان گیری از اطلاعات حساس
- ✓ امن سازی شبکه‌های Wi-Fi
- ✓ پسوردها و احراز هویت؛

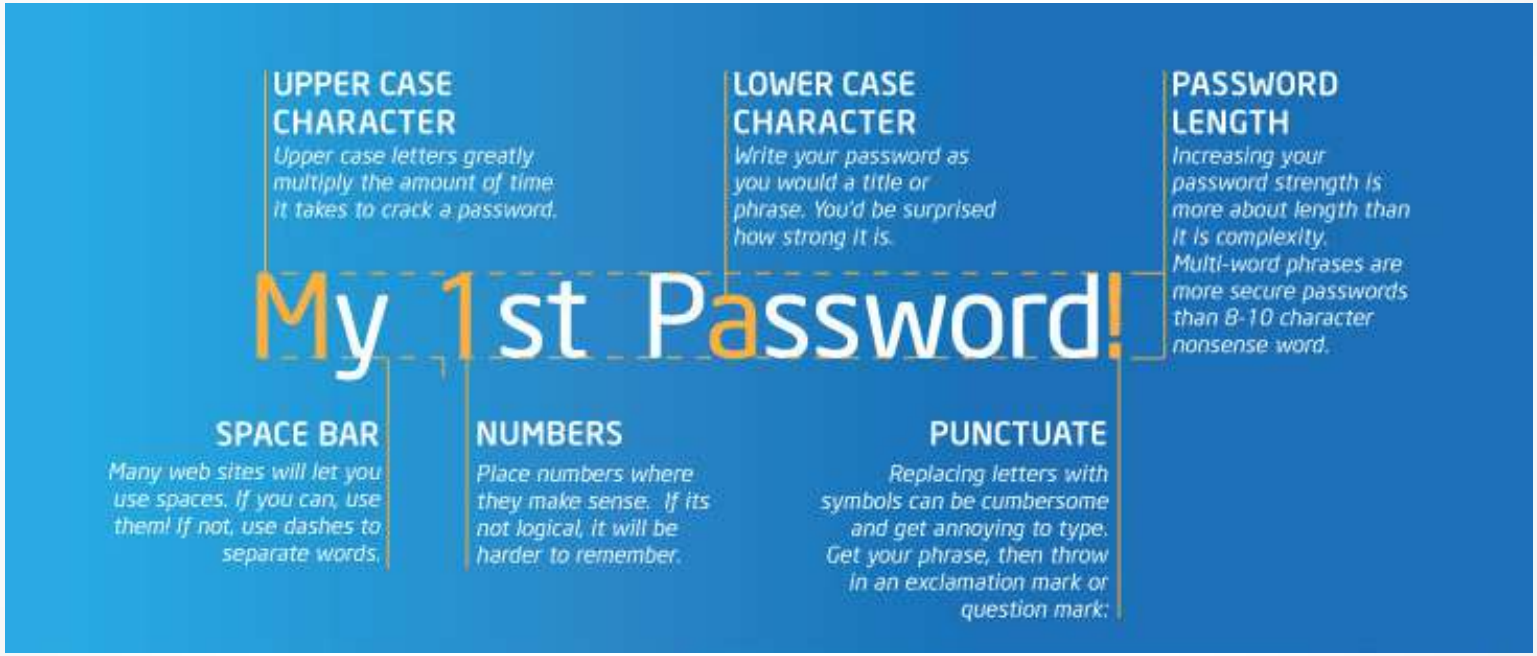
نکات پر مخاطره در استفاده از پسورد

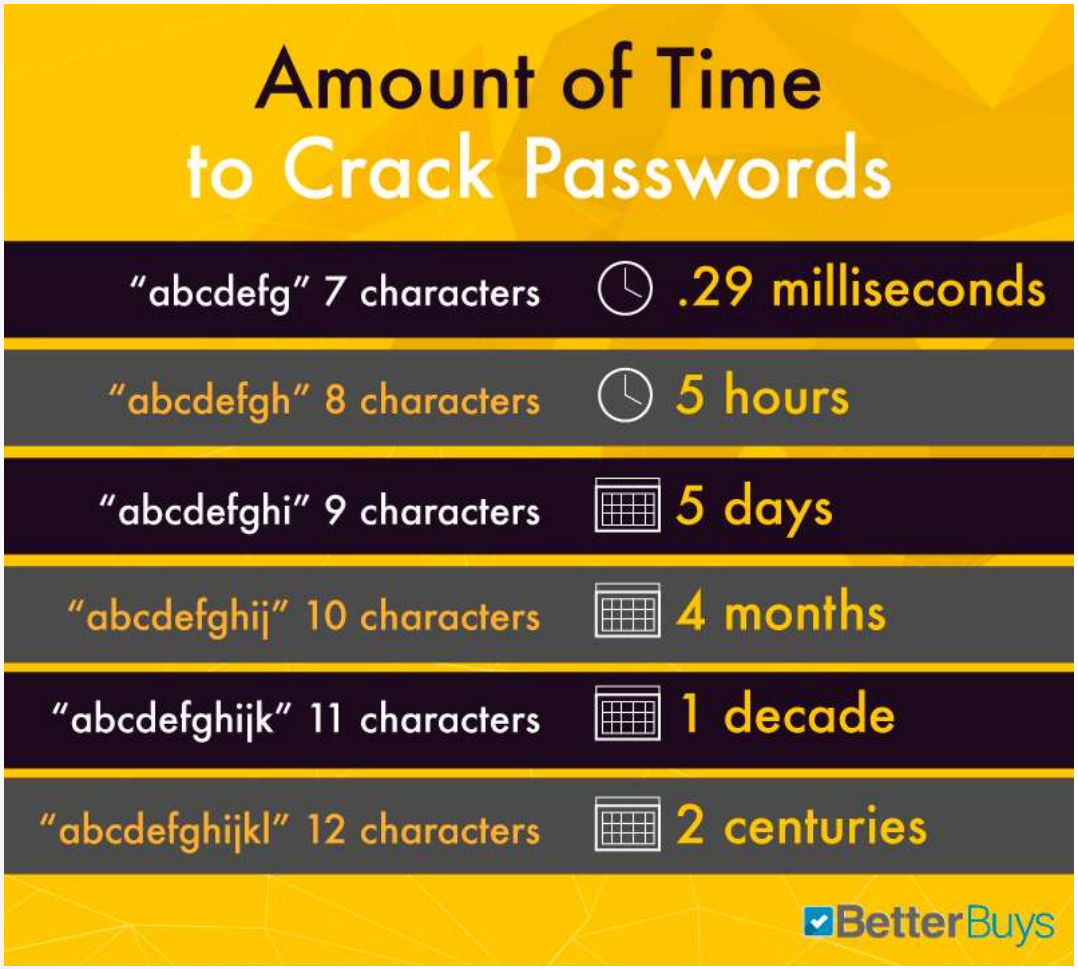


ویژگی های یک پسورد ضعیف



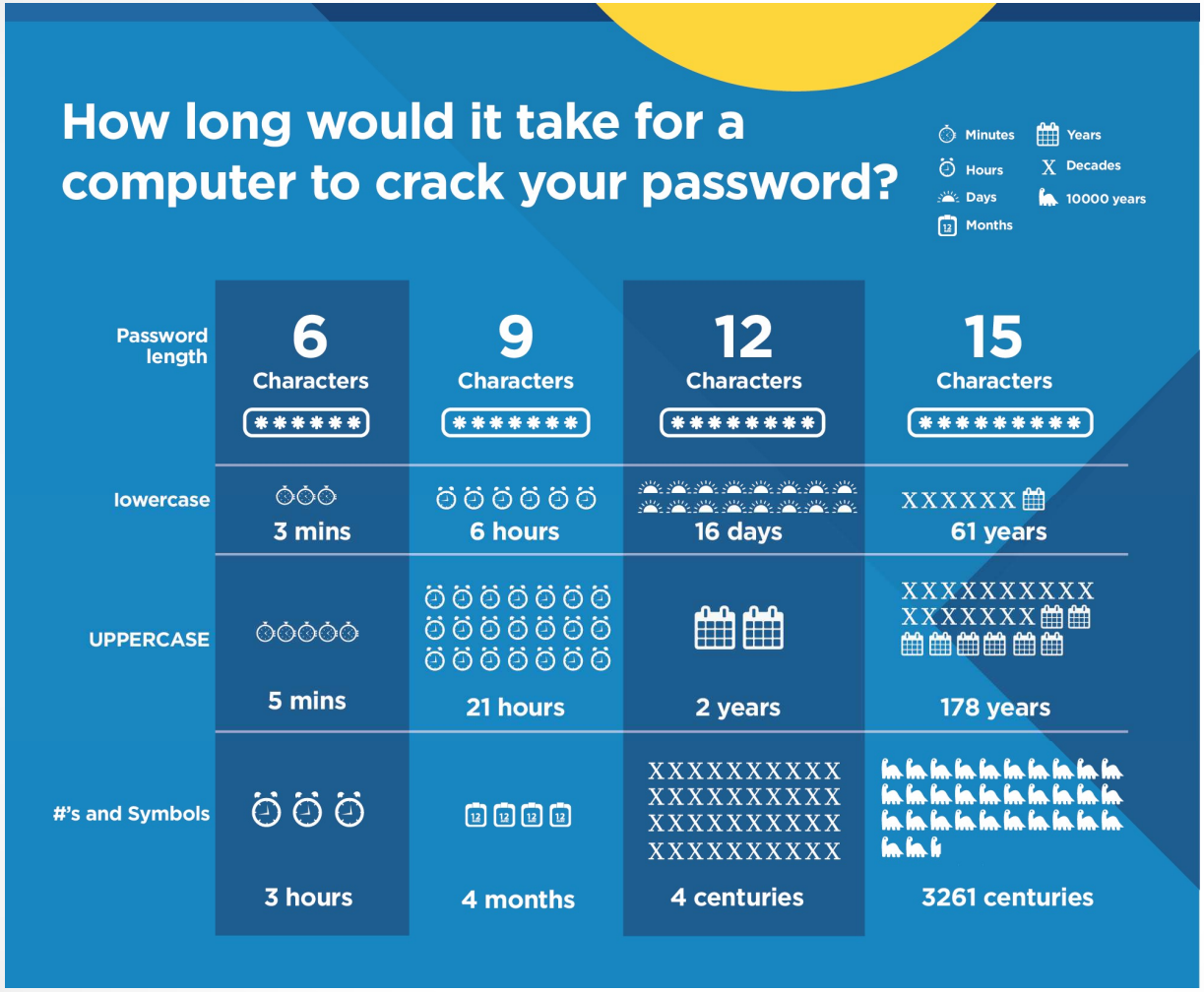
ویژگی های یک پسورد قوی





زمان مورد نیاز برای شکستن یک پسورد

زمان مورد نیاز برای شکستن یک پسورد




مرکز ملی
امنیت سایبری
۱۰ قدم تا
امنیت سایبری
سازمان ملی امنیت سایبری ۱۰ قدم زیر را
برای افزایش امنیت سایبری شما و
شرکتتان پیشنهاد می‌دهد.
مدیریت دسترسی‌های کاربر
دسترسی‌های کامل را محدود کنید.
فعالیت‌های کاربران را مانیتور کنید.
برای کاربران مختلف دسترسی‌های
متفاوت و محدود ایجاد کنید.
مدیریت حادثه
برای بعد از وقوع رخداد
یا حادثه برنامه و سیاست
داشته باشید. برنامه خود
را تست کنید.
جرایم را به مراجع قانونی
اطلاع دهید.
مانیتورینگ
یک روش مانیتورینگ و
سیاست پشتیبانی برای
خودتان داشته باشید.
به صورت مرتب تمام شبکه و سیستم‌ها را
مانیتور کنید. لاگ‌ها و فعالیت‌های غیر
معمول را بررسی کنید.
آزاد کاری
سیاست کار از راه دور داشته
باشید. کارمندانتان را آموزش
دهید که به آن پایبند باشند.
از داده‌ها در ارسال و دریافت
محافظت کنید.
امنیت شبکه
شبکه را نسبت به حمله‌ها امن
کنید. شبکه را مانیتور کنید و
تست‌های امنیتی را انجام دهید.
بالا بردن دانش و آگاهی کاربران
حتما یک سیاست برای کارمندانتان
داشته باشید تا سیستمشان را امن
نگاه دارند. مطمئن شوید که ایشان
را نسبت به تهدیدهای سایبری
آموزش دهید.
جلوگیری از بدافزار
سیاست‌های امنیتی
مربوطه را وضع کنید و
آنتی بدافزار نصب کنید.
کنترل حافظه‌های خارجی
حتما سیاستی برای کنترل و دسترسی
های حافظه‌های خارجی وضع کنید.
قبل ار اتصال این حافظه‌ها به کامپیوتر
حتما آنها را با آنتی ویروس بررسی
کنید.
تنظیمات امنیتی
باگ‌های امنیتی را پچ کنید و
تنظیمات امنیتی کل سیستم را
ست کنید
مدیریت ریسک
سیاست‌های مدیریت ریسک داشته باشید
امنیت سایبری را در الویت قرار دهید
ریسک را ارزیابی کنید
For more information go to www.ncsc.gov.uk @ncsc
ترجمه توسط تیم فنی کنش‌تک - https://koneshtech.academy