



ریاست جمهوری

سازمان مدیریت و برنامه ریزی

مرکز آموزش و پژوهش

امنیت کاربری فناوری اطلاعات (اکفا)

مدرس: مهدی هدایت فر



جلسه چهارم
نهادهای متولی و کار عملی



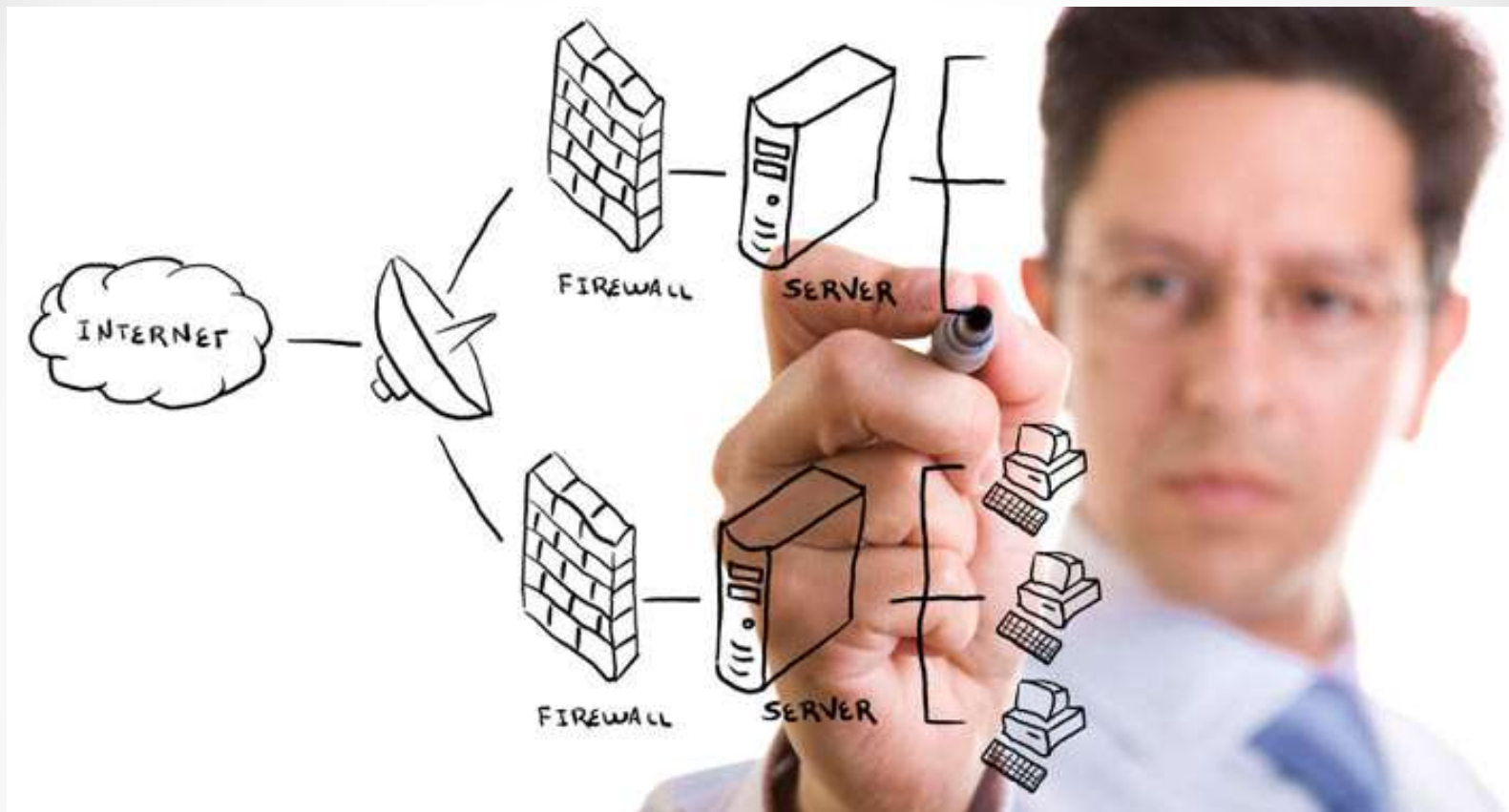
جلسه سوم
روشهای کنترل و مقابله



جلسه دوم
بهداشت سایبری و مفاهیم حقوقی



جلسه اول
مفاهیم امنیت سایبری



روشهای مقابله

قیاس یک شبکه Lan با یک قلعه و یا شهر



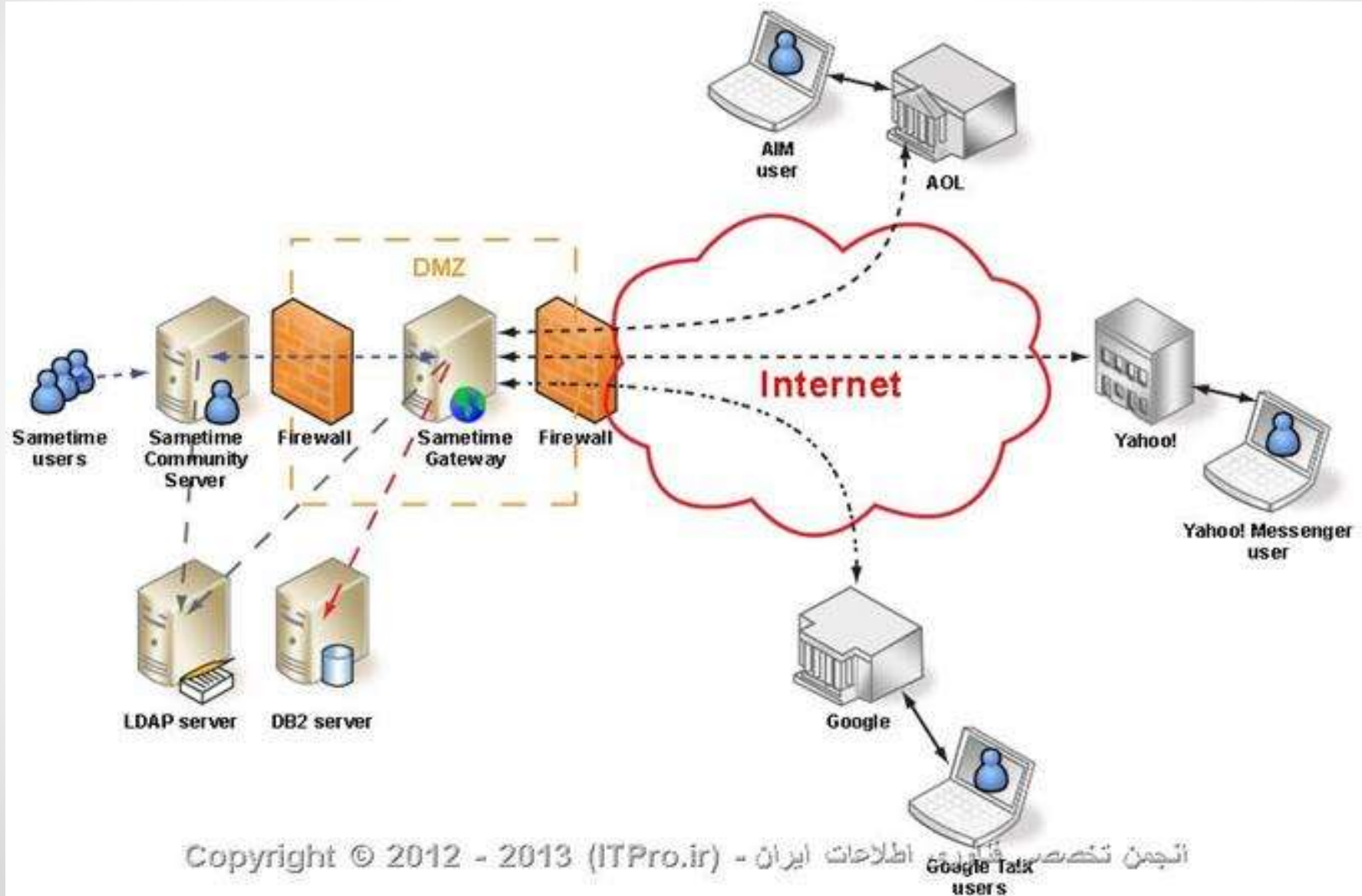
دیوارها: دیواره آتش (Firewalls)

VPN یا Tunnels پل ها: کانالهای ارتباطی)

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



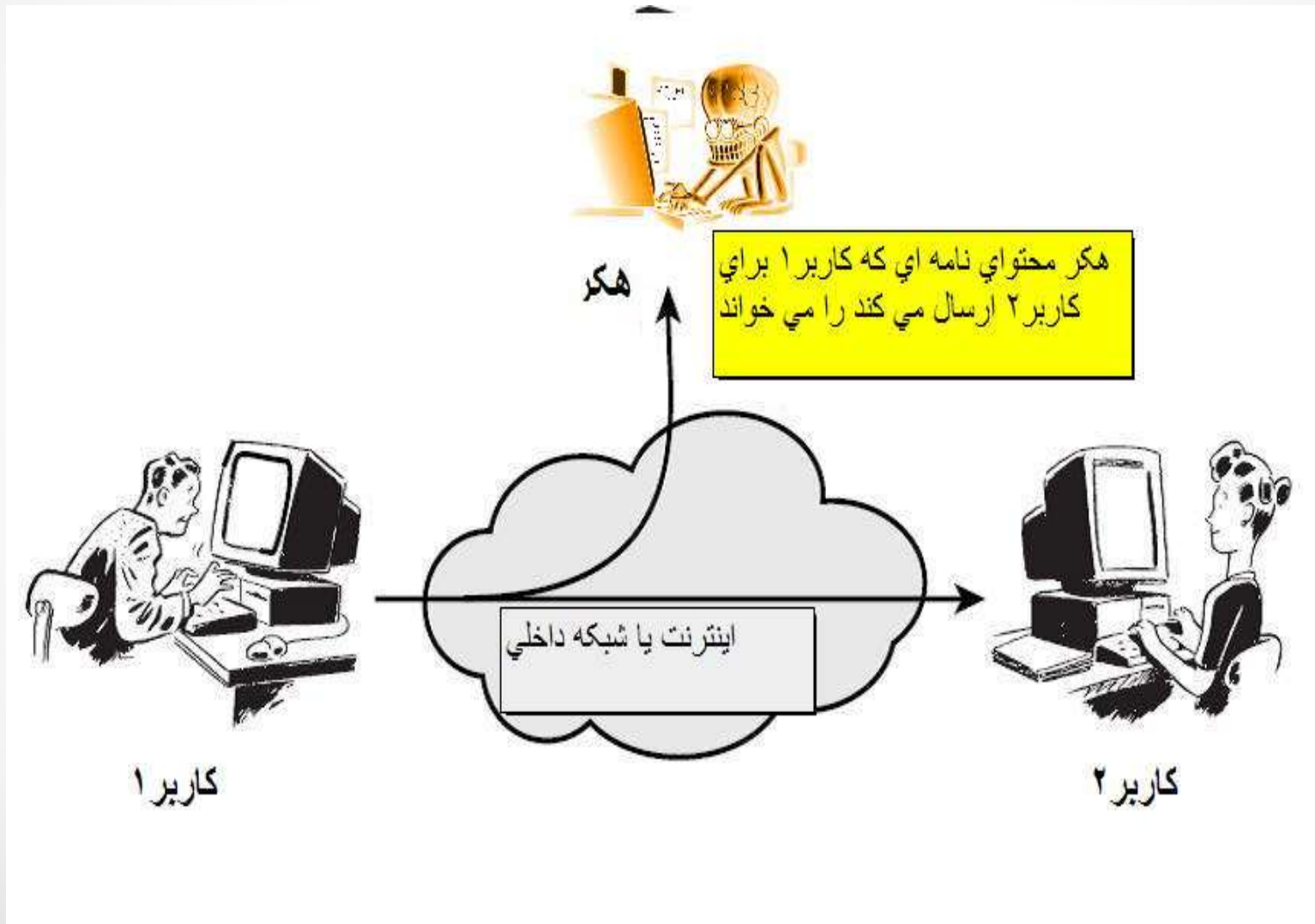
اما نبرد تروا نشان داد این اقدامات کافی نیست



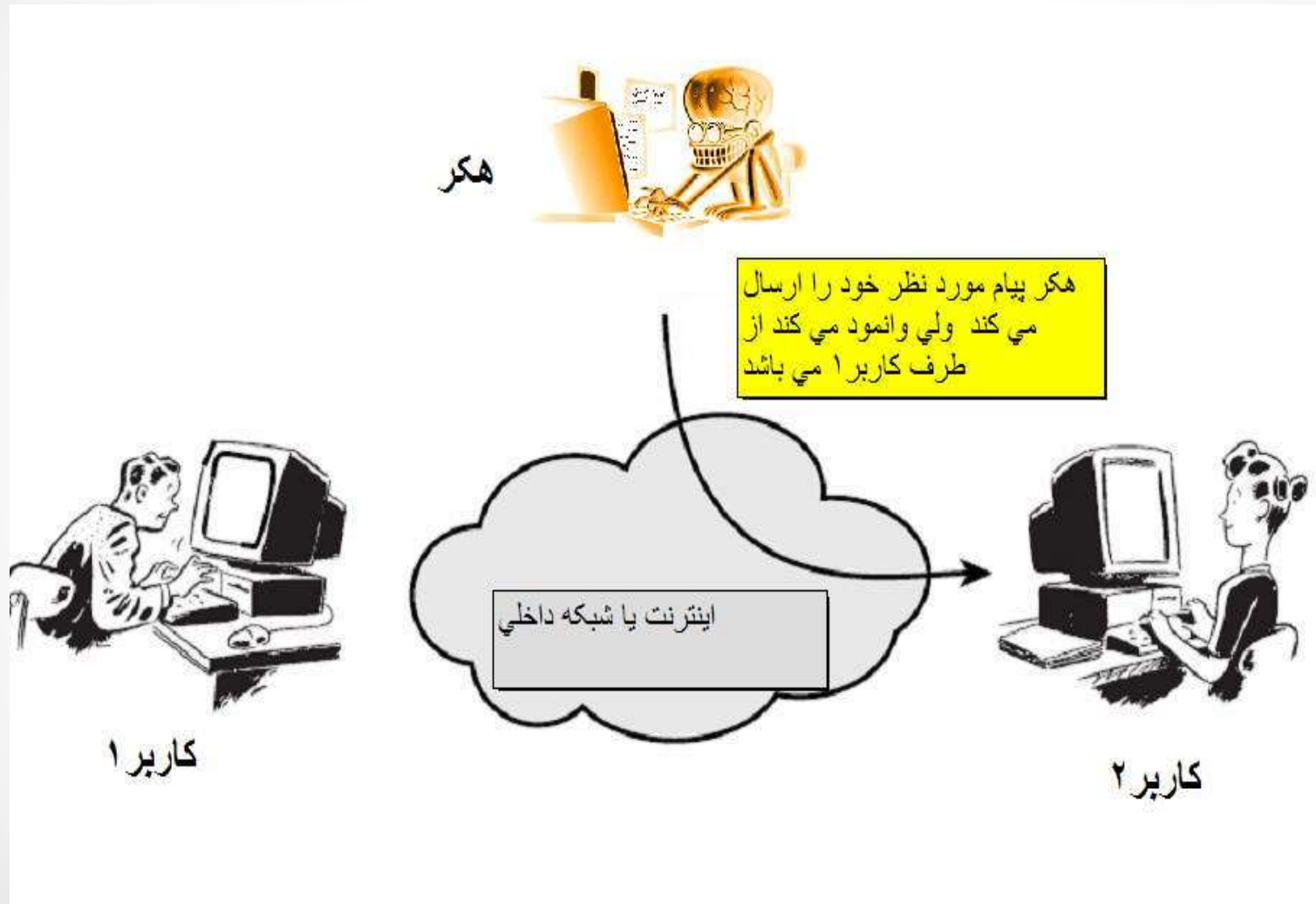
چند نمونه مشابه از نفوذ هکرها به شبکه ها



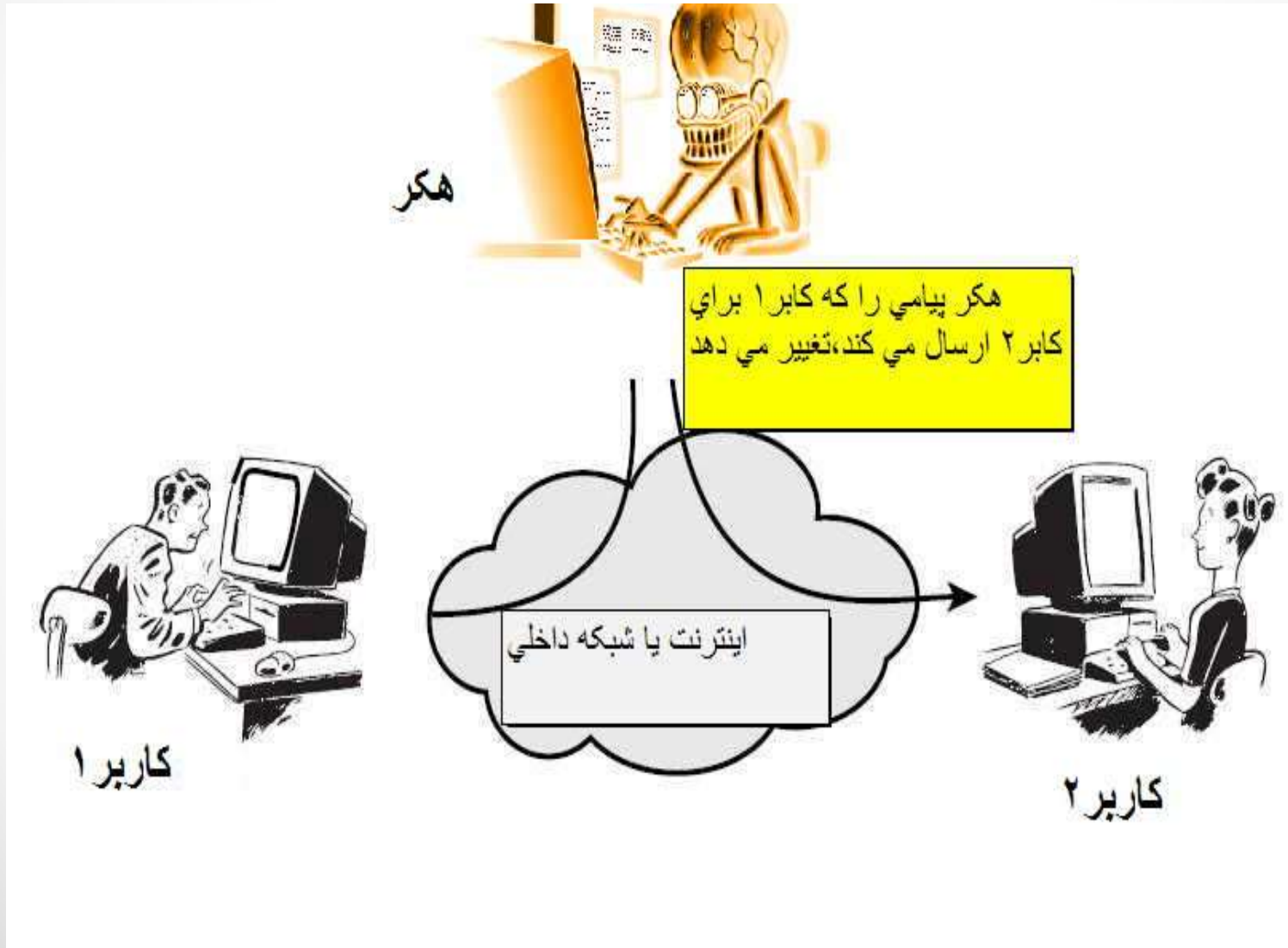
چند نمونه مشابه از نفوذ هکرها به شبکه ها

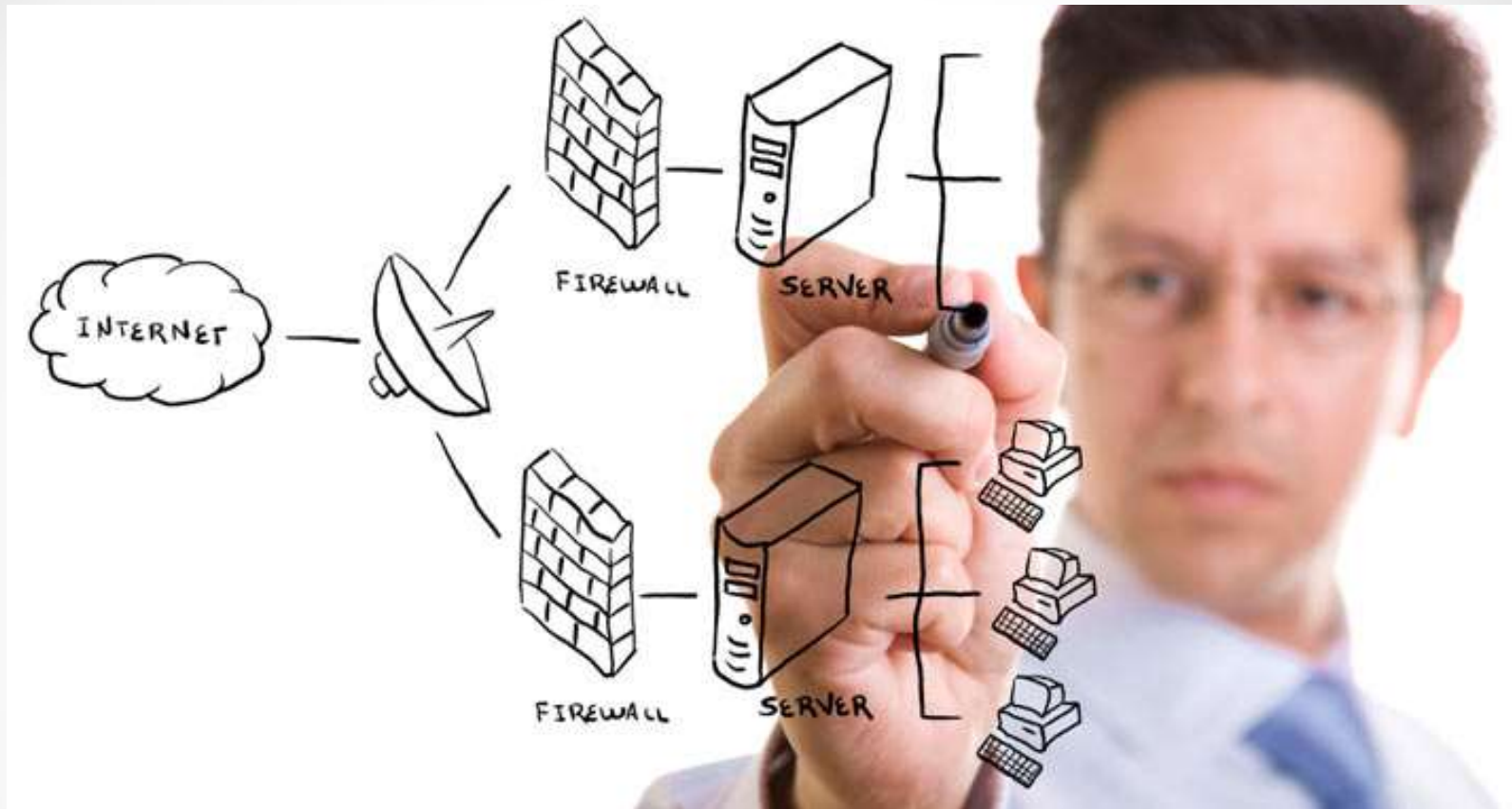


چند نمونه مشابه از نفوذ هکرها به شبکه ها



چند نمونه مشابه از نفوذ هکرها به شبکه ها

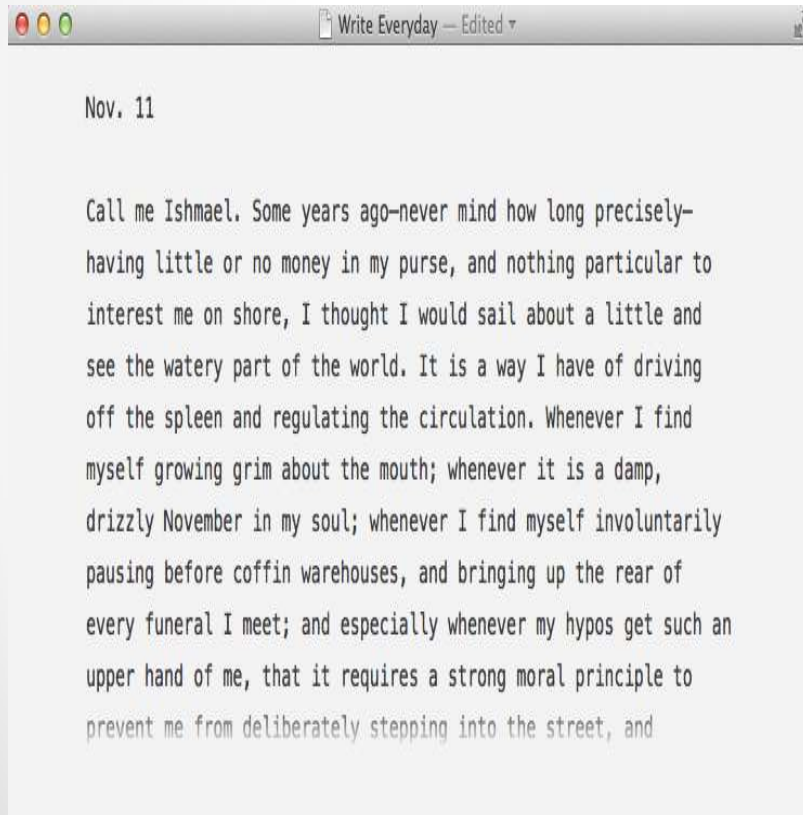




رمزنگاری

چند تعریف در رمزنگاری

متن آشکار Plaintext

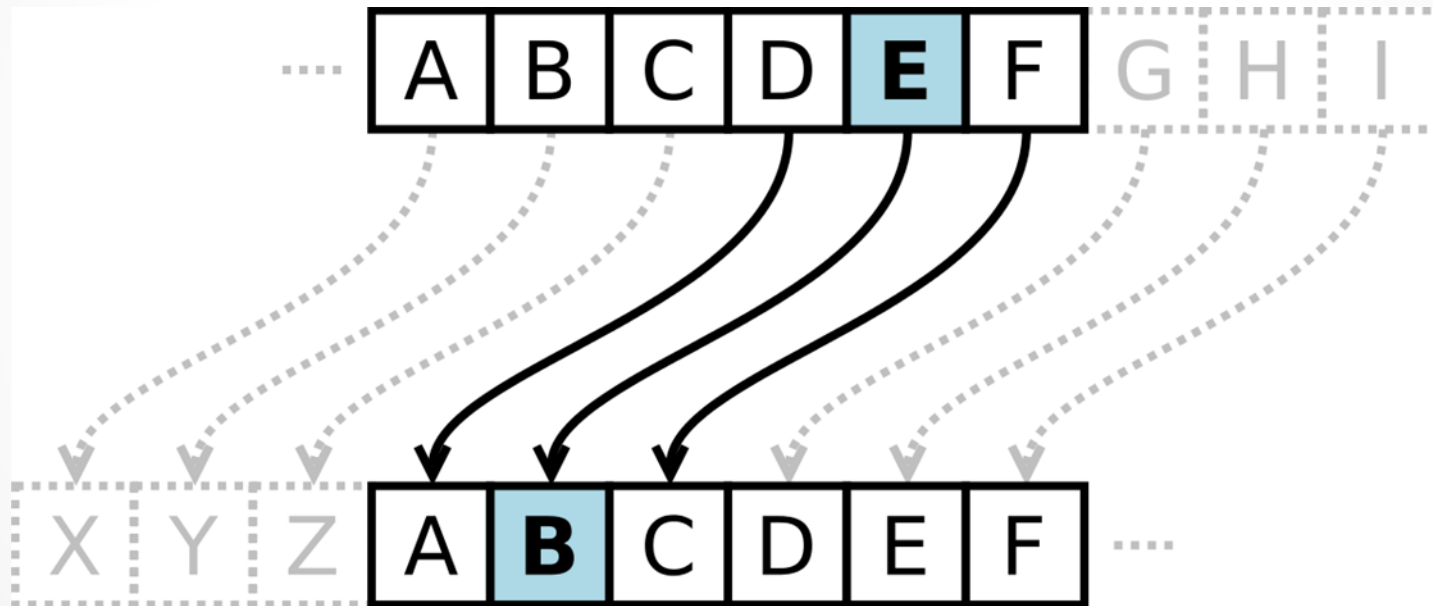


متن رمز Ciphertext

hQIMAw3Jn/nLK/38ARAAsSXLdHctzUYKMptNxZImJXwhhIRm3QxfuyHjJ93ASylE
e+6ABkuyFLJhiKryxp/JmS/alMPfF7hx2aTgovagaPzTwTV1jo6If2mhdCl6keed
1Iz7C0f6jHIqq9d8g0bWDyvELEipn5LNDTX3Xp2Csx5ojRB2wckrUt111Xyj8G0H
4DQUYbINRmJVu1JJc/acGvgOze66pHuRgSCxxHDscefjXenh/XejSYTo7aMi+Es7
DCcd49zH6ZLDQN6BlN9q2oFI8QIhQ2y1QJbat1dWi/4yYwLkZcLKRSm8eo/gNCdL
h9MncXBBSfgbvbu67CDZ9G05geZOn3LzQOpJ8hrZq/6K/uMcUkeZjW3RCo0T754f
E5zYelwUgtwS/lmQ2w5PQF/89bpshtDSYuLlfZgzrsE6DwophuCri5zwCGbEKlsI
g6REIETfbZ2aCL4N2pZVunCIEuoP0zgEB6+M9egdpyxMsMqEBVg3AH7Sa1AtEguP
T/MCxi0bZHCUhPupEKT8slbSrDNxTWMUXQt3XpL0bGCCrDMKLSowYfdiNnRkFbWK
iiqw9hx4Q9CJg7xX7JRnVgwOereIFnMYSbFlvPSxEou6FdBYhdqSefKin4Wnkmdw
qrSl8fjIW/kZ2v72uz0buEKkY9ubBox76yjlRo9KUQMs3em03kc64959gTDiZ0qF
AgwDrosDPQ2BeYQBD/9H5VKFw0an5j5MX1JpOSBAqNGKwq2bcEFnwJfk0DDlhyHD
owHiG7gDowCS+5y/pf56v36HkzpJZATKqoRyKVxmQ0xU913YnPe5fw8iFhxlrfcG
ywzkJh/BRDQ/uy5fhGc/PbSm6iLv/SkkWTK8PSUD+g1yZyK0W7WkMh9QYS20E71Q
qbwPNiy57reWkUWCoE4QmKqqpe7NXXM0eLT912D0hG21thyvTvpskpxszl8+HMJv
M2LMcY2FmmZWAJSdxsQsq9NQdyvCjX2D8oa89WQyXmp7mPXL7BQfoQNPndmn6Obi
0EQojoemRNh14XNhMjPjxw7m34rH2gtvdN3Dg8iFrtocoVJqXqU3N+9T2sNe/bS8

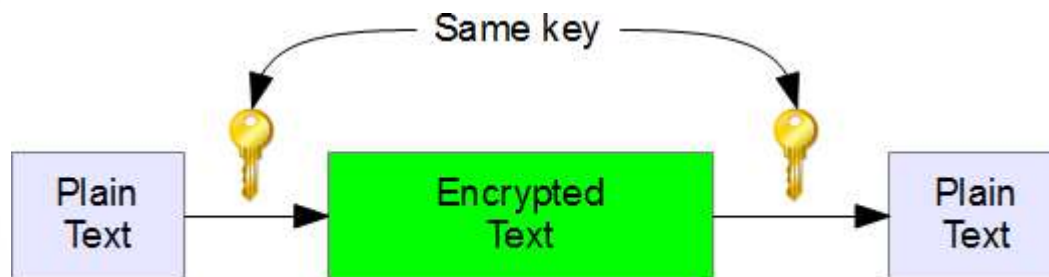
چند تعریف در رمزنگاری

الگوریتم رمزنگاری



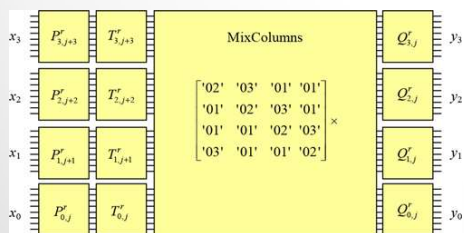
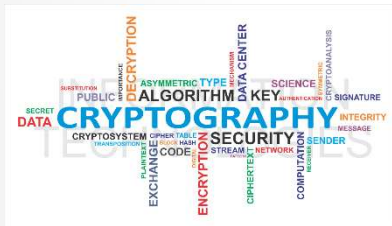
چند تعریف در رمزنگاری

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 Plaintext به Ciphertext

• رمز گشایی (Decipher, Decrypt)

استخراج Plaintext از Ciphertext

• رمز نویسی (Cryptography)

علم اصول روش های encryption

• تحلیل رمز (Cryptanalysis)

علم اصول و روش های Decryption بدون اطلاع از Key که به

آن به اصطلاح codebreaking هم گفته میشود

• رمز نگاری (Cryptology)

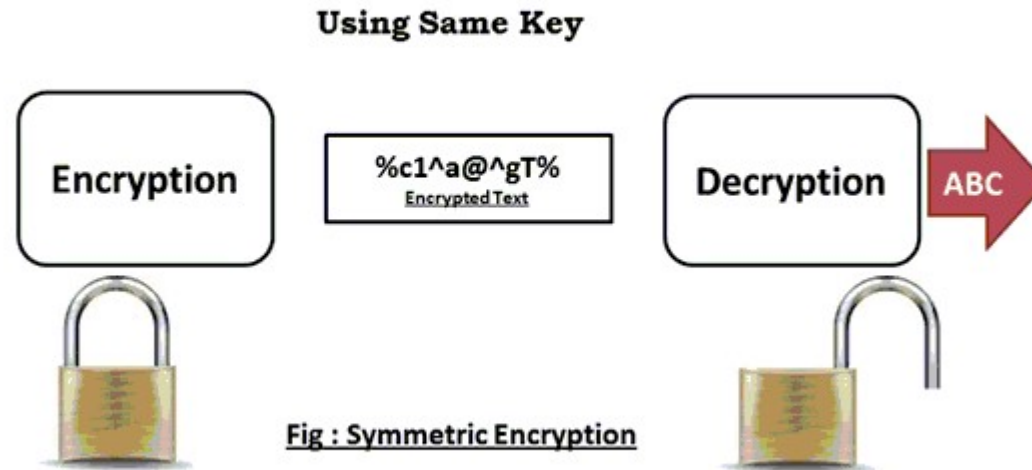
و بالاخره رمز نگاری یعنی علم حاصل از ترکیب

Cryptanalysis و Cryptography



CRYPTOLOGY

رمزنگاری متقارن-Symmetric

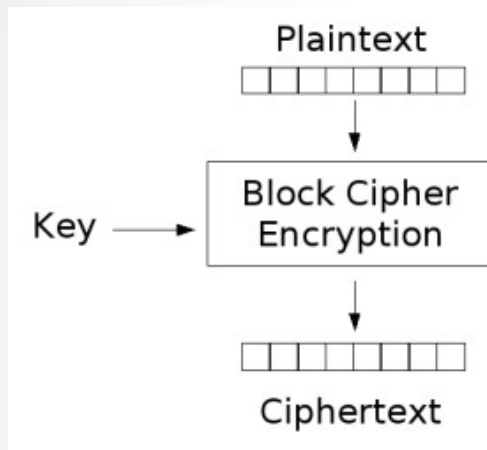


در این روش از کلید مشترک برای Encrypt و Decrypt استفاده میشود از الگوریتم های معروف آن

- 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 AES, 3DES, DES, Blowfish از این نوع هستند

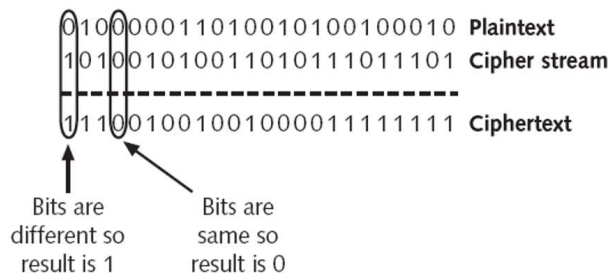


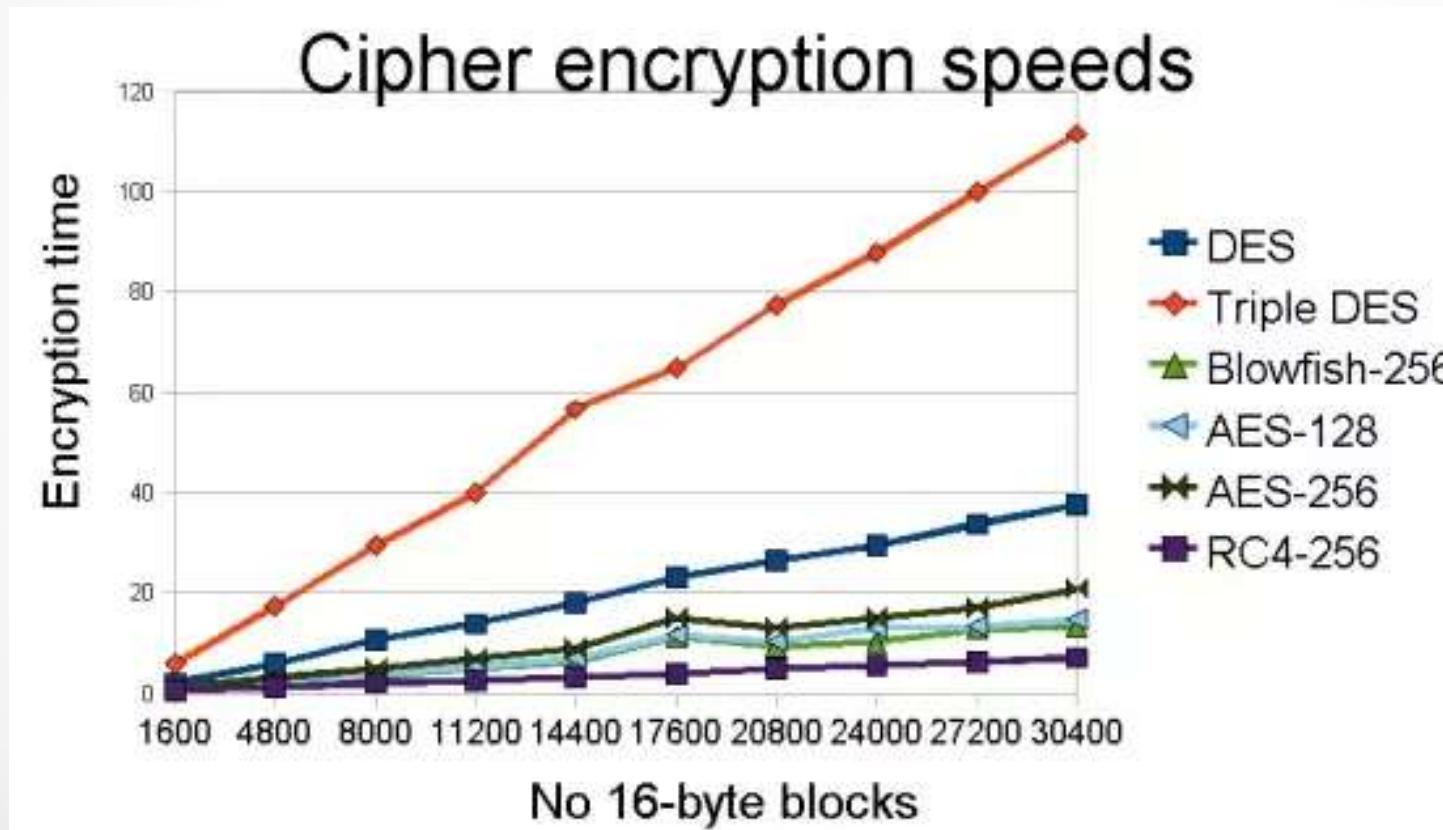
Figure 11-10 Creating ciphertext with XOR

• رمز های جریان ای ((Stream Cipher))

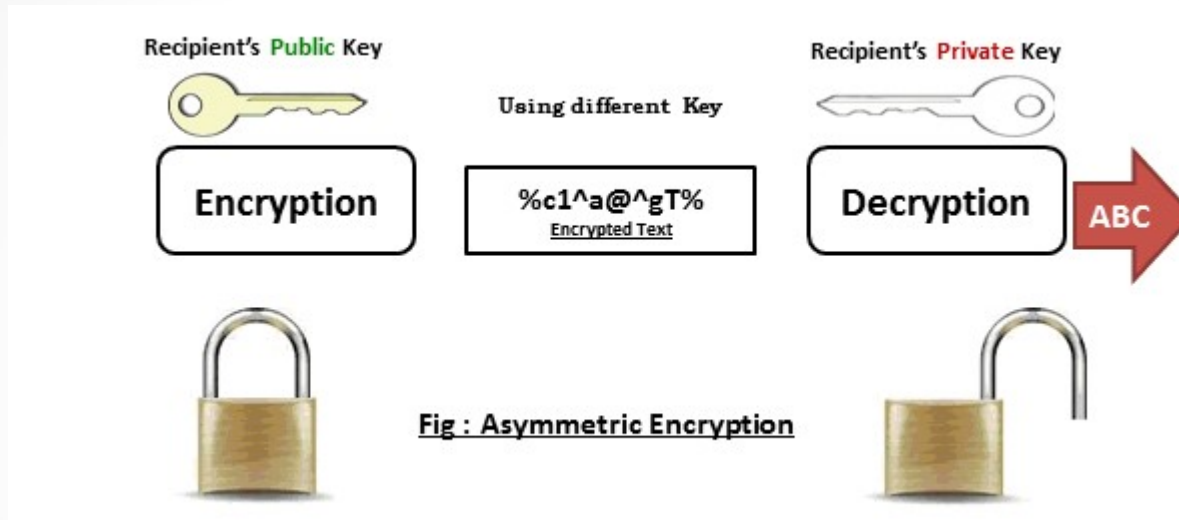
در این نوع پردازش پیام به صورت پیوسته انجام می شود
الگوریتم RC4 از این نوع است

رمزنگاری متقارن-Symmetric

benchmark سرعت الگوریتم های روش متقارن



رمزنگاری نامتقارن-Asymmetric



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 encrypt شده و با private key اطلاعات decrypt میشودز الگوریتم های معروف این روش:

RSA
ElGamal

...

رمزنگاری نا متقارن-Asymmetric

RSA (Rivest–Shamir–Adleman)



رمزنگاری نامتقارن-Asymmetric

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

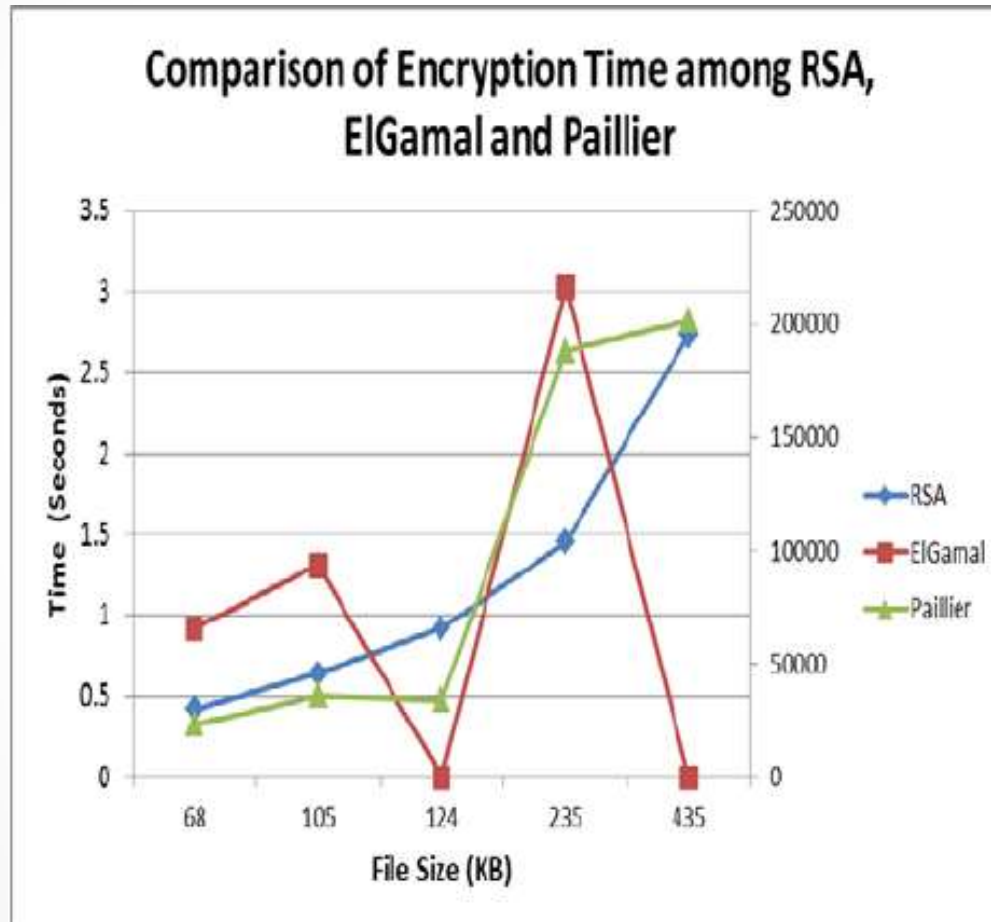
- حل مساله در اختیار داشتن کلید در روش رمزنگاری متقارن
- امضای دیجیتال

ویژگی های روش نامتقارن را میتوان موارد زیر عنوان کرد

- رسیدن به encryption key از decryption key لحاظ محاسبانی ناممکن 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

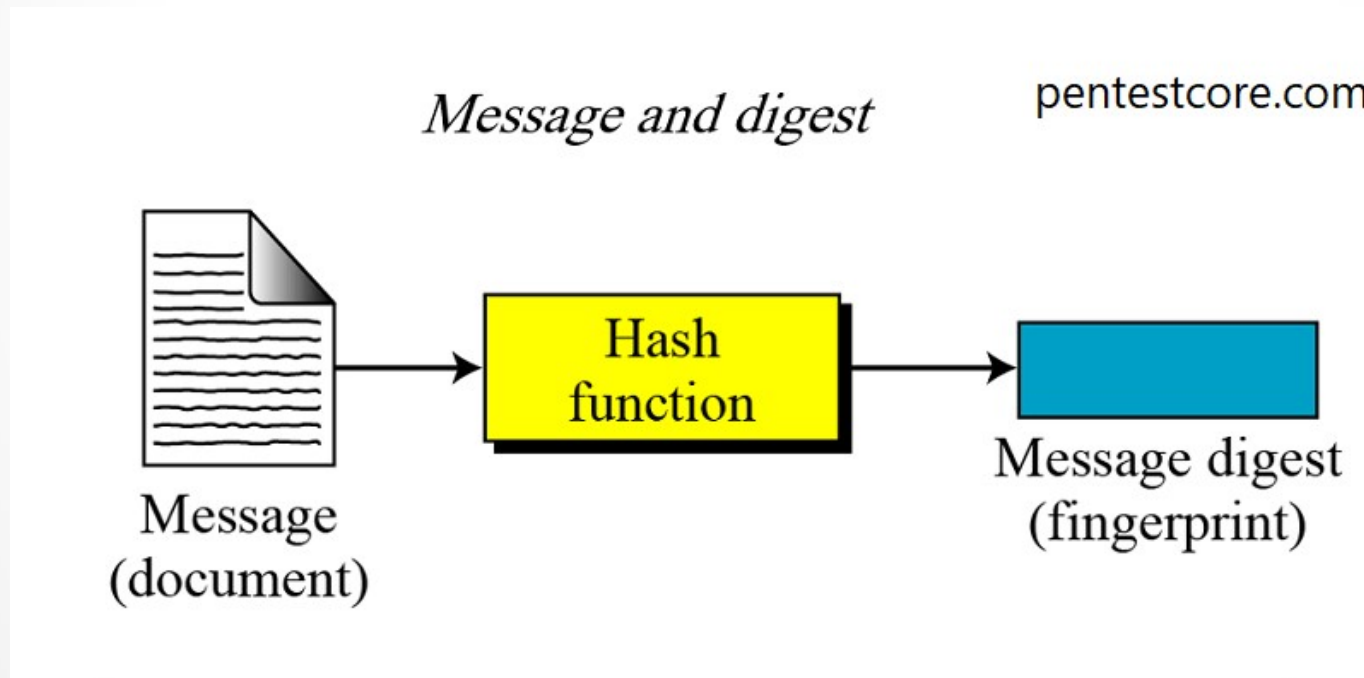
benchmark سرعت الگوریتم های روش نا متقارن



اگر خواستید الگوریتم RSA را امتحان کنید به [اینجا](#) مراجعه کنید البته که قرار شد private key محرمانه 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

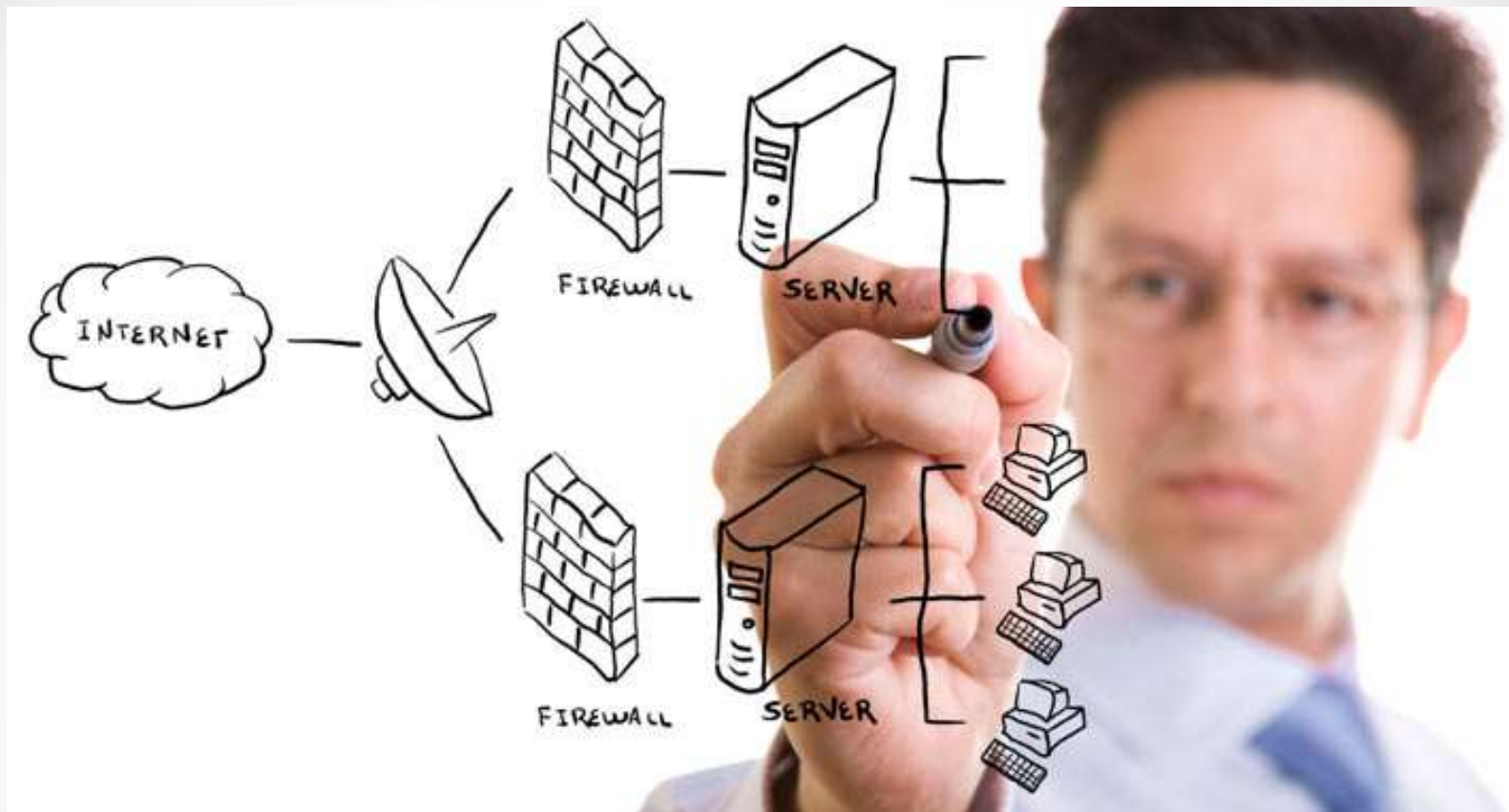
ویژگی ها:

- 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 عبور قوی و حفاظت از آن‌ها؛
- ✓ 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 به صورت رمزنگاری شده باشد؛
- ✓ سهواً یا عمدتاً 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

✓ پشتیبان‌گیری از اطلاعات حساس

✓ امن‌سازی شبکه‌های Wi-Fi

✓ پسوردها و احراز هویت؛



نکات پر مخاطره در استفاده از پسورد

THIEF

UNSECURE NETWORK PASSWORD INTERCEPTION

CODE CRACKING THROUGH WEAK PASSWORDS

SHOULDER SURFING

KEY LOGGING

MOBILE WORKING PASSWORD INTERCEPTION

THEFT

SOCIAL ENGINEERING THROUGH KNOWN INFORMATION

MAIL / PHONE SCAMS

SOCIAL ENGINEERING

No password in place:
too often devices and systems don't actually have a password

Interception:
passwords can be intercepted, particularly is transmitted over an insecure network

Code-cracking:
cyber criminals use sophisticated computer tools to guess billions of passwords until they get in.

Theft:
insecurely stored passwords can be stolen. Don't forget handwritten passwords- if 'hidden' close to a device- or, as we sometimes see - printed onto the case of a laptop or other work device.

Known information:
personal information (often available via social media sites, other security breaches (including of third parties systems), or other social engineering techniques) can facilitate highly targeted manual guessing of passwords

Shoulder surfing:
particularly if you are working in a public place, an alert criminal may well have seen what password you have entered. All that is required then, is for you to leave it unattended, or for your back to be turned, for a few seconds.

Social Engineering:
fraudsters can often persuade people to divulge their passwords. It could be an email or telephone call purporting to be from a bank or your IT team, for example. Many professional firms have been successfully scammed of hundreds of thousands of pounds each, in this way, in 2016 alone.

Key logging:
if your device or systems have been intercepted (eg by someone in the organisation clicking on a malicious link or attachment) a 'keylogger' may have been installed that can track what you are typing into what sites - intercepting all your security controls in the process.

ویژگی های یک پسورد ضعیف

The infographic features a central white padlock icon on the left. To its right are six red circles, each containing a white icon representing a weak password type, with a red diagonal slash through the circle. Below each icon is a text label. The labels are: 'Passwords used previously' (with a padlock icon), 'Your friends' and family members' names' (with a photo of two people), 'Your name or common names' (with a document icon), 'Your login information' (with a form containing 'Username: Admin16', 'Password:', and 'Address: 16'), 'Keyboard patterns & swipes' (with a QWERTY keyboard layout), and 'Single 'dictionary' word (with or without some numbers)' (with a large letter 'A' on a document).

Passwords used previously

Your friends' and family members' names

Your name or common names

Your login information

Keyboard patterns & swipes

Single 'dictionary' word (with or without some numbers)

ویژگی های یک پسورد قوی



Amount of Time to Crack Passwords

"abcdefg" 7 characters  .29 milliseconds

"abcdefgh" 8 characters  5 hours

"abcdefghi" 9 characters  5 days

"abcdefghij" 10 characters  4 months

"abcdefghijkl" 11 characters  1 decade













"abcdefghijkl" 12 characters  2 centuries

 Better Buys

زمان مورد نیاز برای
شکستن یک پسورد

How long would it take for a computer to crack your password?

-  Minutes
-  Hours
-  Days
-  Months
-  Years
-  Decades
-  10000 years

Password length	6 Characters	9 Characters	12 Characters	15 Characters
lowercase	 3 mins	 6 hours	 16 days	 61 years
UPPERCASE	 5 mins	 21 hours	 2 years	 178 years
#s and Symbols	 3 hours	 4 months	 4 centuries	 3261 centuries

زمان مورد نیاز
برای شکستن یک
پسورد



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 کارمندانان 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 از اتصال این حافظه‌ها به کامپیوتر حتما آنها را با آنتی ویروس بررسی کنید.



تنظیمات امنیتی

باگ‌های امنیتی را پیچ کنید و تنظیمات امنیتی کل سیستم را ست کنید



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. کارمندانان را آموزش دهید که به آن پایبند باشند. از داده‌ها در ارسال و دریافت محافظت کنید.

