
ماژول 4

# رمزنگاری

C|SCU
Certified Secure Computer User

Certified Secure Computer User

# Honors & Awards

- MCSA2003-MCSA2003Security
- MCSE2003-MCSE2003Security
- Windows Server 2008 Network Infrastructure Configuration
- Windows Server 2008 Application Infrastructure Configuration
- Windows Server 2008 Active Directory Configuration
- MCITP Server Administrator
- MCITP Enterprise Administrator
- Microsoft Certified Information Technology Professional
- Installing and Configuring Windows Server 2012
- Administering Windows Server 2012
- Configuring Advanced Windows Server 2012 Services
- Microsoft Certified Solutions Associate 2008, 2012
- Microsoft Certified Solutions Expert 2012 - Server Infrastructure
- IT professional - Cyber Security Org – SANS – Cloud Security Org – Network Security Org
- Comptia A+ - Comptia Network + - Comptia Security + - Comptia Master Level Security ( CASP )
- Mcp V1, 2- MCTS
- Microsoft Certified Solutions Expert 2012 - Cloud & Security
- Microsoft Certified Solutions Expert 2012 – MSG

**Best Regards,**

**Alireza Ghahrood**

**Pm: Security Products Manager**

**( Security Solution Provider : Cyber Space |BigData |Cloud |Virtualization**

**Sarv Co**

**Email: Ghahrood.A@Sarvrayaneh.com**

**Tel : +98 ( 21) 88027364 Ext.136 | Cell :+98 (912) 1964383 |**

# آنچه در این فصل می آموزید

استانداردهای رمزنگاری

انواع رمزنگاری

رمزنگاری

ابزارهای رمزنگاری

امضای دیجیتالی

گواهی دیجیتال

# اصطلاحات


متن آشکار
متن رمز شده
کلید رمز


متن آشکار
متن رمز شده
متن رمز شده
متن رمزگشایی شده

# اهداف رمزنگاری

یکپارچگی داده

احراز هویت

عدم انکار

# موارد استفاده رمزنگاری

ذخیره سازی اطلاعات حساس بر روی کامپیوتر بصورت امن

از نام کاربری و پسورد کاربر محافظت می کند

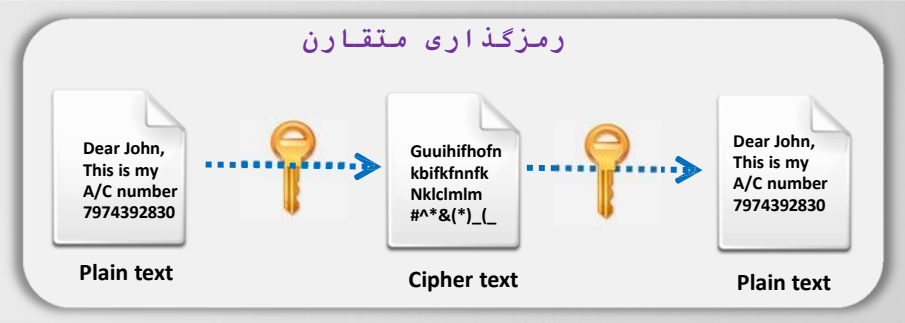
راهی برای ارتباط امن کاربر در شبکه

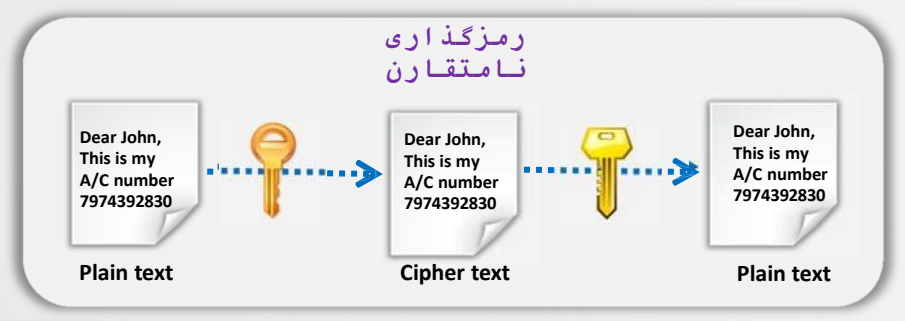
قابلیت سطح بالای اعتماد به هنگام دریافت فایل ها از کاربران دیگربا تضمین قابل اعتماد بودن محتوا و منبع پیام

برای محافظت از اطلاعات تحت وب مثل کارت اعتباری استفاده می شود

هویت فرستنده را ضمانت می کند

# انواع رمز نگاری




کلمه aidin با استفاده از چند الگوریتم hash بصورت زیر در آمده است

| Original text | aidin |
|---|---|
| md2 | d3dadad6dfba098b75d9b12b08a13912 |
| md4 | 4a4c7be4af4efe379820bc3a7bd3d671 |
| md5 | 5aac301f70e5bc4fd7618f785253f821 |
| Sha-1 | 7997037117bdb442a78aa212f19e7748e5d01e88 |
| Sha-256 | ecfa2a327023b205a92ca54969227a5df41f229ac30c78dc9fa9656f2efdd7dc |
| Sha-512 | aa441fe43fb0beeebc44aaf2897774a4b5b0aba75057038932c787a1d9fa1535 bedf798d2ea68489df3e332d2322499dcc386001efc24763015ac46f08cf438f |
| gost | 029ca4887870ba665e7c1e86bf3df780c93a8e2bbafcd44f42a358ababa664d7 |

# استانداردهای رمزگذاری

**Data Encryption Standard (DES)**

**Advanced Encryption Standard (AES)**

# AES

**استاندارد رمزنگاری پیشرفته** مشخصه‌ای برای رمزنگاری داده‌های الکترونیکی است که در سال ۲۰۰۱ توسط مؤسسه ملی فناوری و استانداردهای ایالات متحده ایجاد گردید این رمز که در ابتدا Rijndael نامیده می‌شد، توسط دو رمزنگار بلژیکی به نامهای Joan Daemen و : Vincent Rijmen توسعه داده شد، کسانی که فرایند انتخاب AESرا ارائه نمودند. استاندارد رمزنگاری پیشرفته توسط دولت ایالات متحده پذیرفته شده و اکنون در سراسر جهان استفاده می‌گردد. این الگوریتم رمزنگاری به جای استاندارد رمزنگاری داده‌ها ( (DESکه در سال ۱۹۷۷ منتشر شده ،جایگزین گردیده‌است. الگوریتم استاندارد رمزنگاری پیشرفته یک الگوریتم کلید متقارن است، بدین معنی که از یک کلید یکسان برای رمزنگاری و رمزگشایی استفاده می‌شود.

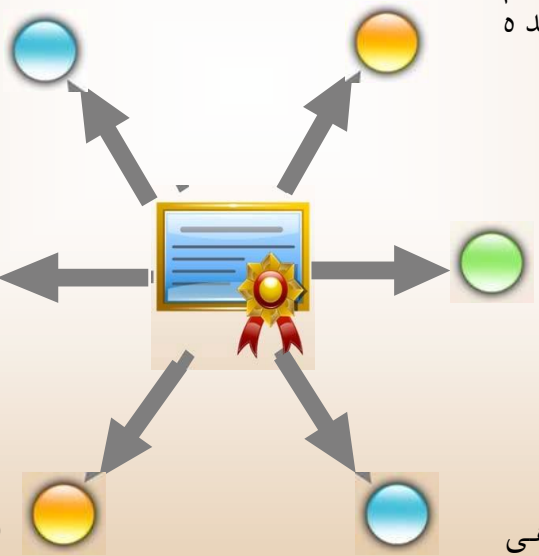
در ایالات متحده، استاندارد رمزنگاری پیشرفته توسط موسسه ملی استانداردها و تکنولوژی به عنوان FIPS PUB 197در نوامبر ۲۰۰۱ اعلان گردید.این اعلان بعد از یک فرایند استانداردسازی پنج ساله بود که در این فرایند ۱۵ طرح، تا قبل از معرفی رمز Rijndaelبه عنوان گزینه مناسب، ارائه و ارزیابی کردید. اگر بخواهیم دقیق شویم، استاندارد AESگونه‌ای از ریندال است که اندازه بلاک آن ۱۲۸ بیتی است.

استاندارد رمزنگاری پیشرفته بر اساس یک قاعده طراحی به نام substitution-permutation networkاست و به هر دو صورت سخت افزاری و نرم‌افزاری سریع است. استاندارد رمزنگاری پیشرفته گونه‌ای از Rijndaelاست که اندازه بلاک ثابت ۱۲۸ بیتی و اندازه کلید ۱۲۸، ۱۹۲ و ۲۵۶ بیتی دارد. در مقابل، مشخصه الگوریتم Rijndaelبا اندازه کلید و اندازه بلاکی تعیین می‌شود که می‌تواند هر ضریبی از ۳۲ بیت، با حداقل ۱۲۸ و حداکثر ۲۵۶ بیت باشد.

# گواهی دیجیتالی

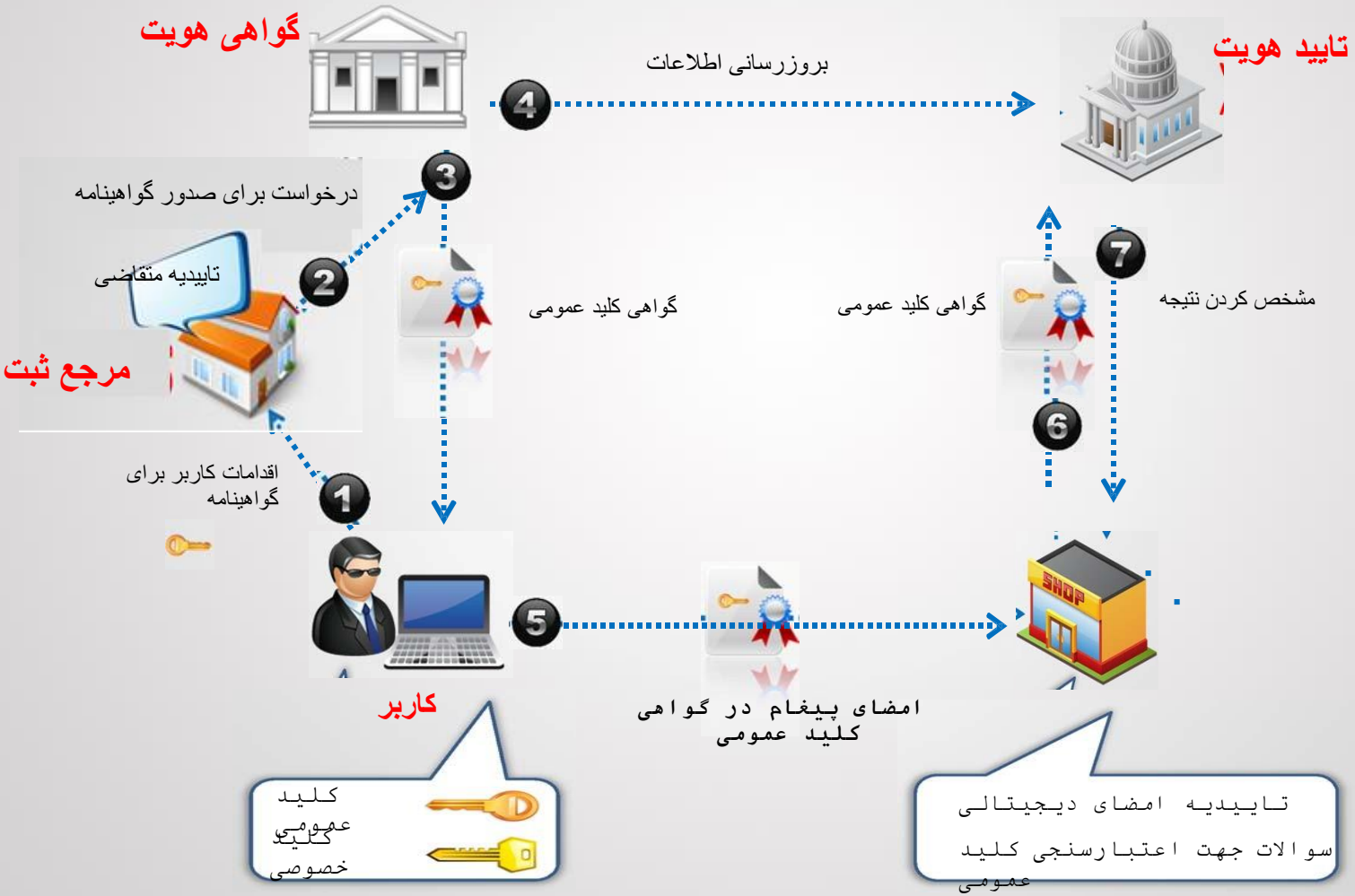
گواهی دیجیتالی کارت های دیجیتالی هستند که برای تایید اطلاعات در تراکنش های آنلاین استفاده می شود

یک گواهی دیجیتالی معمولا شامل موارد زیر می باشد:



- نام سازنده
- جزییات سازنده کلید عمومی
- تاریخ انقضای امضای دیجیتالی
- گواهی هویت امضای دیجیتالی
- نام صادرکننده گواهی هویت
- شماره سریال امضای دیجیتال

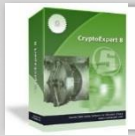
# گواهی دیجیتالی چگونه کار می کند



# ابـزارهـای رمـزنـگـاری

**Advanced Encryption Package Pro**

*http://www.intercrypto.com*



**CryptoExpert**

http://www.cryptoexpert.com/


**GiliSoft File Lock Pro**

http://www.gilisoft.com/

**TrueCrypt**

http://truecrypt.sourceforge.net


**Folder Lock**

*http://www.newsoftwares.net*

**AxCrypt**

http://www.axantum.com/

**Anvide Lock Folder**

**Kruptos 2 Professional**

http://www.kruptos2.co.uk/

**BoxCryptor Unlimited**

**All In One Protector Premium Plus**

**USB Secure**

http://www.newsoftwares.net/

**Password Protect Video Master**

# SSL چیست؟