به نام خدا

دانشکده مهندسی برق،
دانشگاه صنعتی شریف

مبانی رمزنگاری و امنیت شبکه

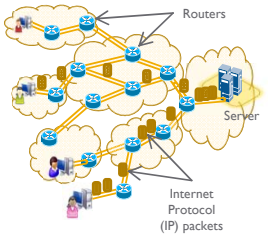
مقدمه، مرور کلی مفاهیم رمزنگاری و مبانی نظری

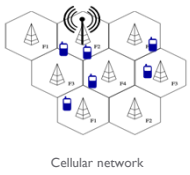
Introduction, Basic Concepts of Cryptography and preliminaries

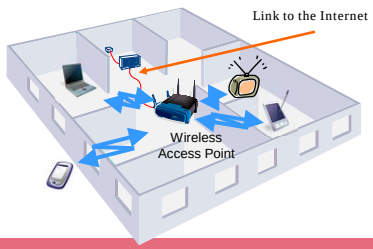
مهتاب میرمحسنی

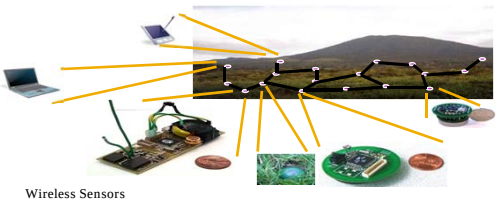
نیم‌سال دوم (بهار) ۹۸-۹۹

امنیت در سیستم‌های شبکه‌ای









۲

محتوای درس

- مقدمات
  - اهداف امنیتی و مدل‌های حمله

- الگوریتم‌ها و پروتکل‌های رمزنگاری
  - رمزنگاری متقارن و نامتقارن برای ایجاد محرمانگی (Confidentiality)
  - الگوریتم‌های یکپارچگی داده (Data Integrity)
  - پروتکل‌های احراز اصالت (Authentication)

- امنیت شبکه
  - عمدتاً بر پایه روش‌های رمزنگاری
  - پیشگیری، آشکارسازی و تصحیح موارد نقض امنیت

Security is much more than cryptography! ۳

سرفصل مطالب

- مقدمه، مرور کلی مفاهیم رمزنگاری و مبانی نظری
- سیستم‌های رمز دنباله‌ای یا جریانی
- سیستم‌های رمز قالبی
- سیستم‌های کلید همگانی (نامتقارن)
- توابع چکیده‌ساز، کدهای احراز اصالت پیام و امضای دیجیتال
- مدیریت کلید در سیستم‌های رمزنگاری
- پروتکل‌های احراز اصالت
- مدل‌های کنترل دسترسی
- سازو کارها و پروتکل‌های امنیتی در شبکه
  - امنیت لایه transport (SSL; TLS; HTTPS; SSH)
  - امنیت پست الکترونیکی (PGP و S/MIME)
  - امنیت داده در حال انتقال (امنیت IP و پروتکل IPSec)
  - سیستم‌های تشخیص نفوذ (IDS و Honeypot)
  - کنترل دسترسی به شبکه (فایروال‌ها)

- Introduction, Basic Concepts of security goals, adversary & attacks, and preliminaries
- Stream Ciphers
- Block Ciphers
- Public Key Cryptography
- Hash Functions, Message Authentication Codes and Digital Signature
- Key Management and Distribution
- User Authentication Protocols
- Access Control Models
- Network and internet Security
  - Transport level security: SSL; TLS; HTTPS; SSH
  - Email Security (PGP and S/MIME)
  - Security of Transient Data (IP Security and IPSec)
  - Intrusion Detection Systems
  - Access Control in Networks (Firewalls)

۴

سرفصل مطالب

در صورت امکان:

- حملات لایه فیزیکی مانند اخلال
- امنیت بی‌سیم
  - امنیت لایه transport بی‌سیم: 802.11; WEP; WAP;
  - احراز اصالت: Kerberos; TLS; PEAP
- حریم خصوصی
  - نیازمندی‌ها، طراحی با حفظ حریم خصوصی، PGP; Mix-Nets; Onion routing
- امنیت در اینترنت اشیا و فناوری‌های نوظهور
  - شبکه های حسگری
  - محاسبات امن
  - مدل اعتماد بر پایه زنجیره قالب‌ها
- توافق کلید در لایه فیزیکی برای اینترنت اشیا

Time permitting (Perhaps in projects):

- Physical layer attacks: Jamming and jamming-perpetrated attacks
- Wireless security
  - 802.11; Wired Equivalent Privacy (WEP); Wireless Application Protocol (WAP); Wireless transport layer security
  - Authentication: Kerberos; TLS; PEAP
- Privacy and privacy enhancing technologies
  - Requirements; Privacy by design; PGP; Mix-Nets; Onion routing; Location privacy protection
- Security for emerging networks and Internet of Things (IoT)
  - Pervasive computing and wireless sensor networks
  - Secure and private computation methods
  - Block-chain based trust model
- Physical-layer key agreement for IoT

۵

نحوه ارزیابی

- تکالیف + تکالیف کامپیوتری ۱۵٪
- پروژه ۵٪ +
- امتحان میان‌ترم ۳۵٪ -چهارشنبه ۹۹/۲/۱۷
- امتحان پایان‌ترم ۵۰٪ - یکشنبه ۹۹/۴/۱

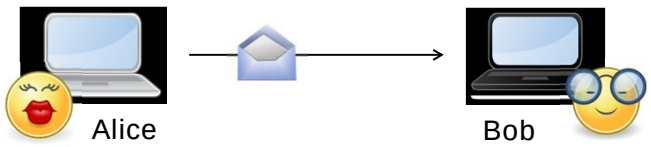
۶

مراجع

- William Stallings, Cryptography and Network Security Principles and Practices, 7th Edition, Pearson, 2016.

1. Matt Bishop, Computer Security: Art and Science, Addison-Wesley, 2003.
2. D. Robling Denning Cryptography and Data Security, Addison-Wesley, 1982.
3. H. Beker and F. Piper, Cipher System, Northwood Books, 1982.
4. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th Edition, 2005.

Why security?



- Alice wants to communicate with Bob
- What could possibly go wrong?

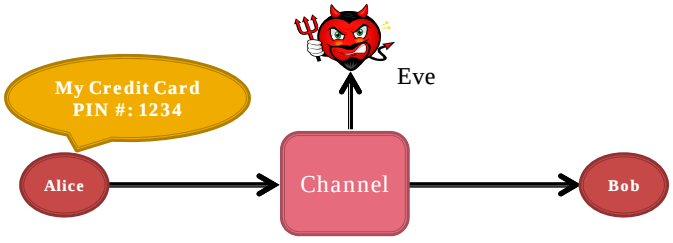
امنیت
Computer Security

- NIST (National Institute of Standards and Technology)
- **نیازمندی‌های امنیتی**: تحقق سه ویژگی زیر در منابع اطلاعاتی سیستم (CIA triad)
  - محرمانگی (Confidentiality)
  - یکپارچگی یا تمامیت (Integrity)
  - دسترس‌پذیری (Availability)
    - تضمین دسترسی به موقع افراد مجاز به خدمت

۹

محرمانگی (Confidentiality)

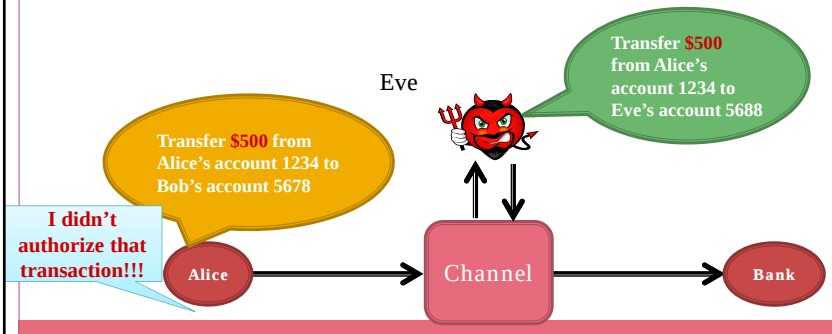
- محرمانگی داده: عدم افشای داده‌های محرمانه یا خصوصی
- حریم خصوصی (Privacy): کنترل حریم داده‌ها توسط افراد



۱۰

یکپارچگی یا تمامیت (Integrity)

- تضمین عدم دستکاری (modification)، اصالت یا اعتبار (authenticity) و انکارناپذیری (non-repudiation)
  - یکپارچگی داده: عدم تغییر داده‌ها و برنامه‌ها توسط افراد غیر مجاز
  - یکپارچگی سیستم: عدم دستکاری عمدی یا غیرعمدی سیستم توسط افراد غیر مجاز



۱۱

نیازمندی‌های امنیتی +

- احراز اصالت **Authentication**
  - Verify who you are (Proof of identity)
  - Verify a trusted source
  - Validity of a transmission, a message, or message originator

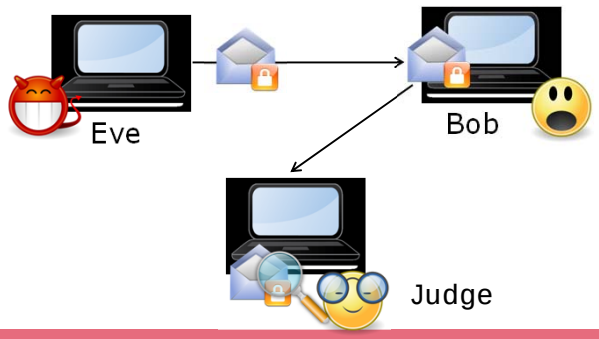
- مجاز شناسی **Authorization**
  - Manage rights to perform a task

- پاسخگویی (ممیزی-حسابرسی)**Accountability (Auditing)**
  - Tracking of the performed task
    - Logging/Forensic analysis . Analysis . Billing
  - nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, after-action recovery and legal action.

۱۲

نیازمندی‌های امنیتی +

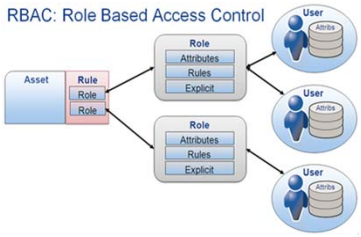
- انکار ناپذیری Non Repudiation
  - Nobody else can manipulate our data -
  - We cannot deny the content -
  - Both origin and destination •



۱۳

نیازمندی‌های امنیتی +

- کنترل دسترسی Access Control
  - Authentication
  - Authorization
  - Monitor (audit)
- حریم خصوصی Privacy
  - گمنامی Anonymity
  - پیوندناپذیری Unlinkability
  - Unobservability
  - Pseudonymity



۱۴

مشکلات برقراری امنیت

- برخلاف نیازمندی‌ها، ساز و کارهای مورد نیاز جهت تامین آن‌ها پیچیده است.
- معمولا حملات موفق از دیدگاه جدیدی به الگوریتم‌ها نگاه می‌کنند.
- جایگاه استفاده از ساز و کارهای امنیتی مختلف، متفاوت است.
- پیاده‌سازی ساز و کارهای امنیتی دشواری‌هایی از جمله توزیع اطلاعات امن (مانند کلید مخفی)، ملاحظات جدید پروتکلی و ... دارد.
- مهاجم (attacker) کافی است که تنها یک ضعف سیستم را بیابد ولی طراح می‌بایست همه ضعف‌ها را یافته و از بین ببرد.

۱۵

مشکلات برقراری امنیت

- پیش از شکست امنیتی، اهمیت آن برای کاربران و مدیران سیستم روشن نیست.
- برقراری امنیت نیاز به نظارت دایمی دارد.
- ملاحظات امنیتی در طراحی اولیه سیستم‌ها در نظر گرفته نشده است.
- برقراری امنیت به عنوان مانعی در برابر کارآیی در نظر گرفته می‌شود.

۱۶

ساختار امنیتی OSI

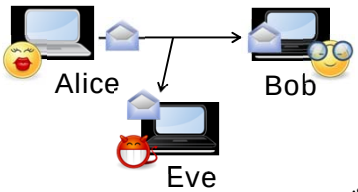
- تعریف سیستماتیک نیازمندی‌های امنیتی و روش‌های ارضای آن‌ها
- ITU-T X.800 “Security Architecture for OSI”

- حمله امنیتی (Security attack)
  - عملی که امنیت اطلاعات سازمان را تهدید می‌کند.
- ساز و کار امنیتی (Security mechanism)
  - فرآیندی که برای پیشگیری، تشخیص و بازیابی از حملات امنیتی طراحی شده است.
- خدمات امنیتی (Security service)
  - خدمات مخابراتی یا پردازشی که با استفاده از یک یا چند ساز و کار امنیتی به مقابله با حملات امنیتی می‌پردازند.

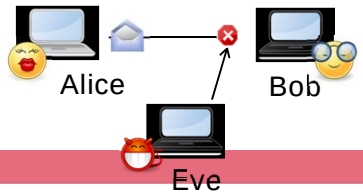
۱۷

حملات امنیتی
Security attacks

- مهم‌ترین تقسیم‌بندی حمله‌ها (از نظر هدف مهاجم - متخاصم Adversary)
- حمله غیرفعال Passive attack
  - توسط شنود(eavesdropping) صورت می‌گیرد و منابع سیستم را تغییر نمی‌دهد.



- حمله فعال Active attack
  - حمله‌ای است که سعی در تغییر منابع یا کارکرد آن‌ها دارد.

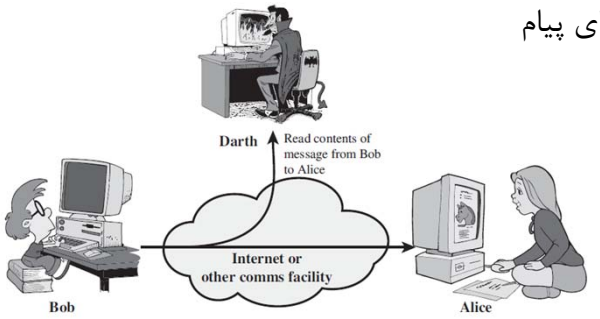


۱۸

حمله غیرفعال
Passive attack

- شنود (Wiretapping-eavesdropping) یا پایش (monitoring)
- هدف: بدست آوردن اطلاعات ارسالی

1. بدست آوردن محتوای پیام

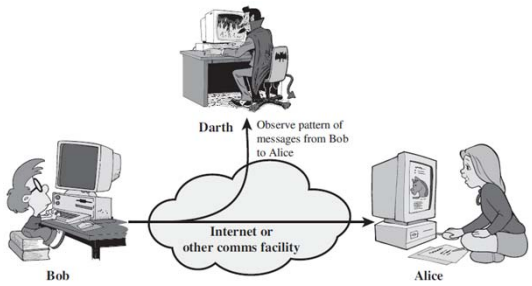


(a) Release of message contents

۱۹

حمله غیرفعال (ادامه)

2. تحلیل ترافیک
   - Sniffing



(b) Traffic analysis

- آشکارسازی بسیار مشکل
- پیشگیری با استفاده از رمزنگاری

۲۰

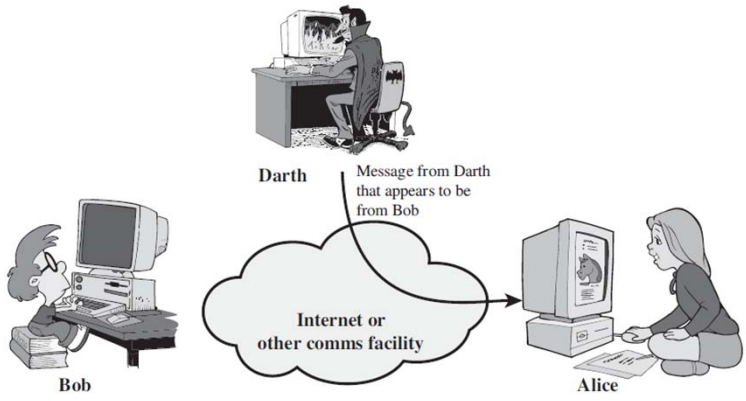
حمله فعال
Active attack

- تغییر دنباله داده و یا تولید دنباله غلط
  1. حمله رخ‌پوشی (masquerade)
  2. حمله تکرار (replay)
  3. حمله تغییر پیام (modification of messages)
  4. حمله منع خدمت (denial of service)
  5. حمله اخلال Jamming
  6. ...
- پیشگیری مشکل: تنوع آسیب‌پذیری‌های ممکن
- هدف: آشکارسازی و بازیابی

۲۱

حمله رخ‌پوشی
masquerade

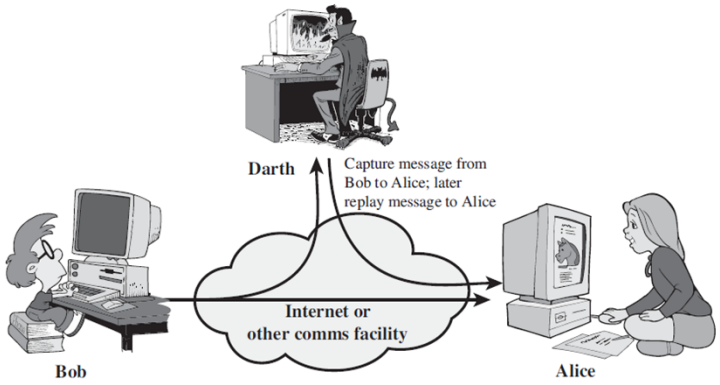
- ادعای هستار (entity) دیگر



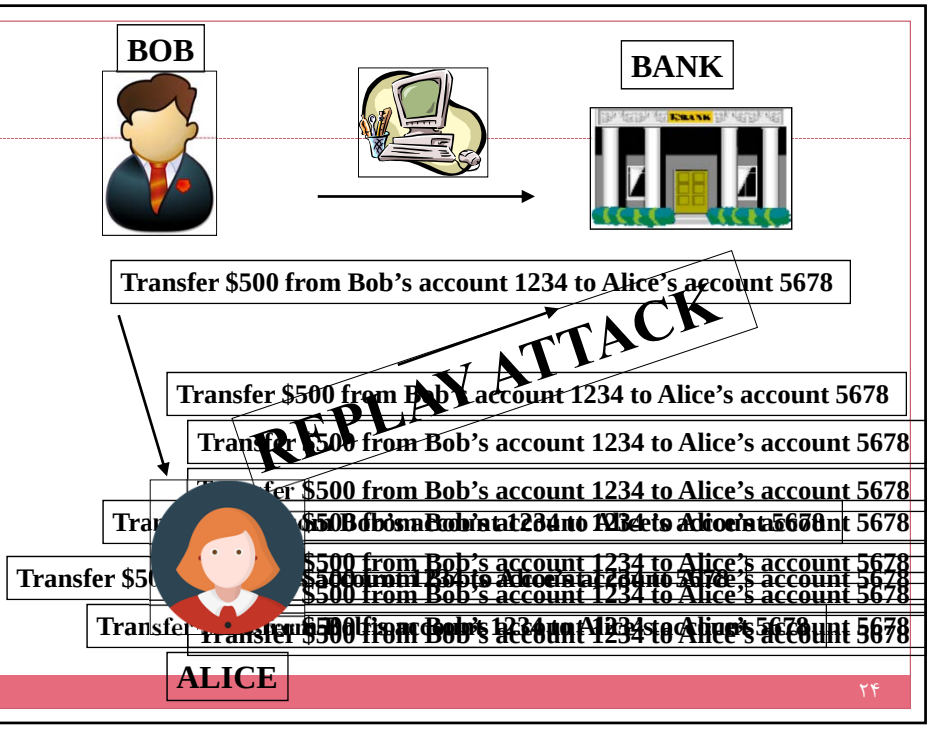
۲۲

حمله تکرار
replay

- بدست آوردن داده (غیرفعال) و ارسال‌های غیر مجاز بعدی



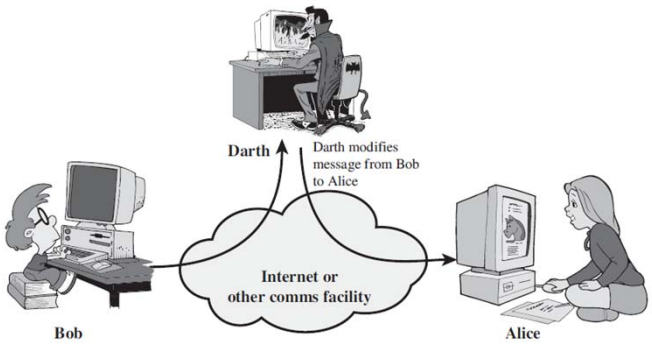
۲۳



۲۴

حمله تغییر پیام
modification of messages

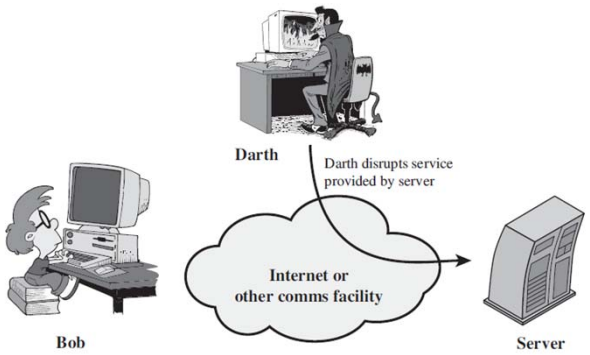
- تغییر کل یا قسمتی از پیام، تاخیر و یا تغییر ترتیب غیر مجاز
- حمله فرد در میانه (Man in the middle)



۲۵

حمله منع خدمت
(DoS) denial of service

- هدف مشخص: مانند تمامی پیام‌های ارسالی به یک گیرنده مشخص
- کل شبکه: سیل ترافیکی یا حمله به ضعف‌ها



۲۶

خدمات امنیتی
Security services

- X.800: ۵ گروه و ۱۴ خدمت امنیتی
  - احراز اصالت (Authentication)
  - کنترل دسترسی (Access Control)
  - محرمانگی داده (Data Confidentiality)
  - یکپارچگی داده (Data Integrity)
  - انکارناپذیری (Non-repudiation)

۲۷

احراز اصالت
Authentication

- احراز اصالت هستار همتا (Peer Entity Authentication)
  - ارتباط با اتصال
- اتصال:
  - احراز اصالت هستار همتا در شروع اتصال
  - مقابله با حمله رخ‌پوشی و تکرار در طول اتصال
- احراز اصالت مبدا پیام (Data-Origin Authentication)
  - ارتباط بدون اتصال
  - مثال: email، ...
- پیام منفرد: احراز اصالت مبدا پیام

۲۸

کنترل دسترسی
Access Control

- پیشگیری از استفاده غیر مجاز منابع
- کنترل افراد مجاز، شرایط مجاز و نحوه استفاده افراد مجاز
- محدود و کنترل کردن دسترسی به منابع میزبان از طریق یال‌های مخابراتی

- ابتدا: احراز اصالت هستارها
- سپس: تعیین دسترسی‌ها

۲۹

محرمانگی داده
Data Confidentiality

- محافظت از داده‌ها + شار ترافیک در برابر حملات غیرفعال
- رمزنگاری

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

۳۰

یکپارچگی داده
Data Integrity

- اطمینان از دریافت دقیقا آنچه که فرستنده مجاز ارسال کرده است
- ارتباط با اتصال
  - مقابله با تغییر، واردکردن، حذف و یا تکرار

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

- دو دسته سرویس امنیتی:
  - بازیابی بعد از حمله
  - تشخیص حمله
- کد احراز اصالت پیام، امضا

۳۱

یکپارچگی داده
Data Integrity

- ارتباط بدون اتصال
- مقابله با تغییر یا دستکاری پیام (modification)

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

- دو دسته سرویس امنیتی:
  - بازیابی بعد از حمله
  - تشخیص حمله

۳۲

انکارناپذیری
Non-repudiation

- پیشگیری از انکار پیام ارسالی در **فرستنده** و **گیرنده**
  - امضا

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

- **دسترس‌پذیری (Availability)**
  - منابع سیستم بر اساس تقاضای افراد مجاز (احراز اصالت شده) قابل دسترسی باشند
  - در X.800 این خاصیت را متصل به سایر خدمات تعریف کرده است.

۳۳

ساز و کارهای امنیتی
Security mechanism

- در یک لایه خاص:
- رمزگذاری (Encipherment): الگوریتم ریاضی + کلید
- امضای دیجیتال (Digital Signature)
- کنترل دسترسی (Access Control)
- یکپارچگی داده (Data Integrity)
- تبادل داده برای احراز اصالت (Authentication Exchange)
- لایه‌گذاری ترافیکی (Traffic Padding): مقابله با تحلیل ترافیک
- کنترل مسیریابی (Routing Control): انتخاب مسیرهای امن
- رسمی‌سازی (Notarization): استفاده از شخص ثالث معتمد (trusted third party)

۳۴

رابطه خدمات امنیتی و ساز و کارهای امنیتی

	Mechanism							
Service	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer Entity Authentication	Y	Y			Y			
Data Origin Authentication	Y	Y						
Access Control			Y					
Confidentiality	Y						Y	
Traffic Flow Confidentiality	Y					Y	Y	
Data Integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

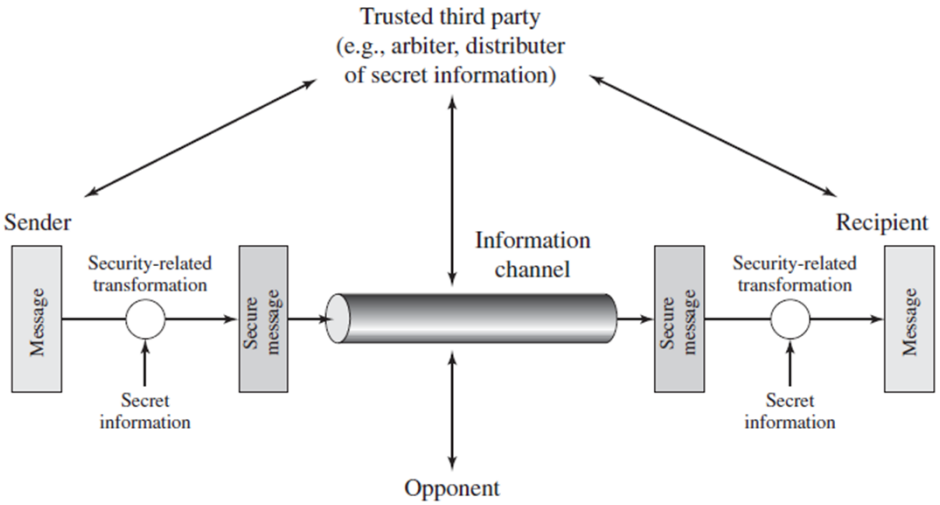
۳۶

اصول طراحی سیستم‌های امن

- Economy of mechanism: ساده‌ترین و سبک‌ترین طراحی ممکن – شانس کمتر حمله مهاجم
- Fail-safe defaults: اعطای کنترل دسترسی بر پایه اجازه نه حذف – تشخیص خطای پیاده‌سازی
- Complete mediation: به روزرسانی خق دسترسی و پخش آن در شبکه ...
- Open design
- Separation of privilege: احراز اصالت چند فاکتوره
- Least privilege
- Psychological acceptability: حفظ کارآیی سیستم
- Isolation

۳۷

مدل امنیت شبکه



۳۸

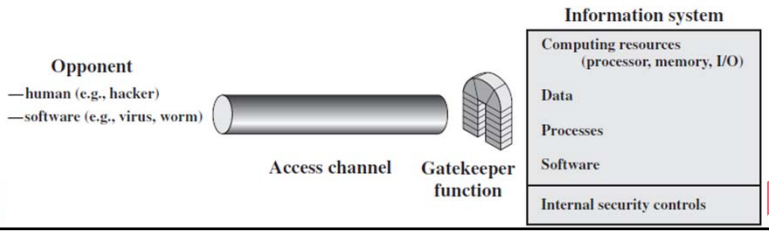
طراحی خدمت امنیتی

1. طراحی الگوریتم مناسب برای اعمال امنیت
2. تولید اطلاعات مخفی مورد نیاز الگوریتم (مانند کلید)
3. راهکارهای توزیع و توافق درباره اطلاعات مخفی
4. طراحی پروتکل مناسب برای استفاده از موارد فوق جهت تضمین هدف خاص امنیتی

۳۹

مدل امنیتی دسترسی شبکه

- رخنه‌گر (hacker)، نفوذگر (intruder)
1. تهدید دسترسی اطلاعات (Information access threats)
2. تهدید خدمات (Service threats)
- دسترسی فیزیکی یا از طریق **شبکه**
- دروازه نگهدار (gatekeeper)
  - استفاده از گذرواژه
  - کنترل‌های داخلی برای تشخیص نفوذ



۴۰

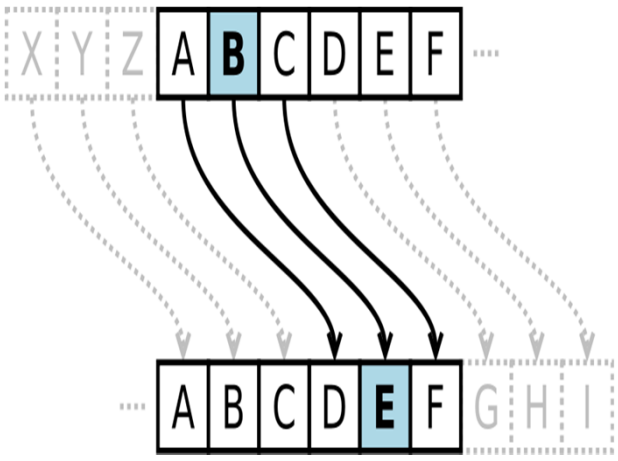
رمزنگاری

تاریخچه رمزنگاری

- مرحله اول: تا آغاز قرن بیستم
  - استفاده از سیستم‌های ساده جانشینی و جابجایی ساده (مانند سیستم سزار و سیستم اسپارتا)
  - قلم، کاغذ و ماشین‌های ساده مکانیکی
- مرحله دوم: از آغاز قرن بیستم تا آغاز دهه ۱۹۵۰
  - وسایل پیچیده مکانیکی و الکترومکانیکی و به تبع آن سیستم‌های رمزنگاری پیچیده‌تر
- مرحله سوم:
  - شروع با انتشار مقالات بسیار مهم شانون در سال‌های ۱۹۴۸ و ۱۹۴۹ و پیشرفت سریع در صنایع میکروالکترونیک در دهه ۱۹۶۰
- مرحله چهارم:
  - شروع از اواخر دهه ۱۹۷۰ با پیشنهاد سیستم‌های رمزنگاری با کلید همگانی
  - رمزنگاری مدرن
- مرحله پنجم: از آغاز دهه ۱۹۹۰: همگانی شدن علم رمزنگاری

۴۲

رمز سزار Caesar Cipher



۴۳

سیستم اسپارتا –رمز استوانه‌ای

۴۴

پایه علم رمز

- نظریه اطلاعات (Information Theory)
- نظریه کدگذاری (Coding Theory)
- نظریه پیچیدگی (Complexity Theory)
- نظریه اعداد (Number Theory)
- جبر (Algebra)
- آمار و فرآیندهای تصادفی (Statistics and Stochastic Processes)
- علوم کامپیوتر (Computer Science)
- الکترونیک

۴۵

تعاریف اساسی

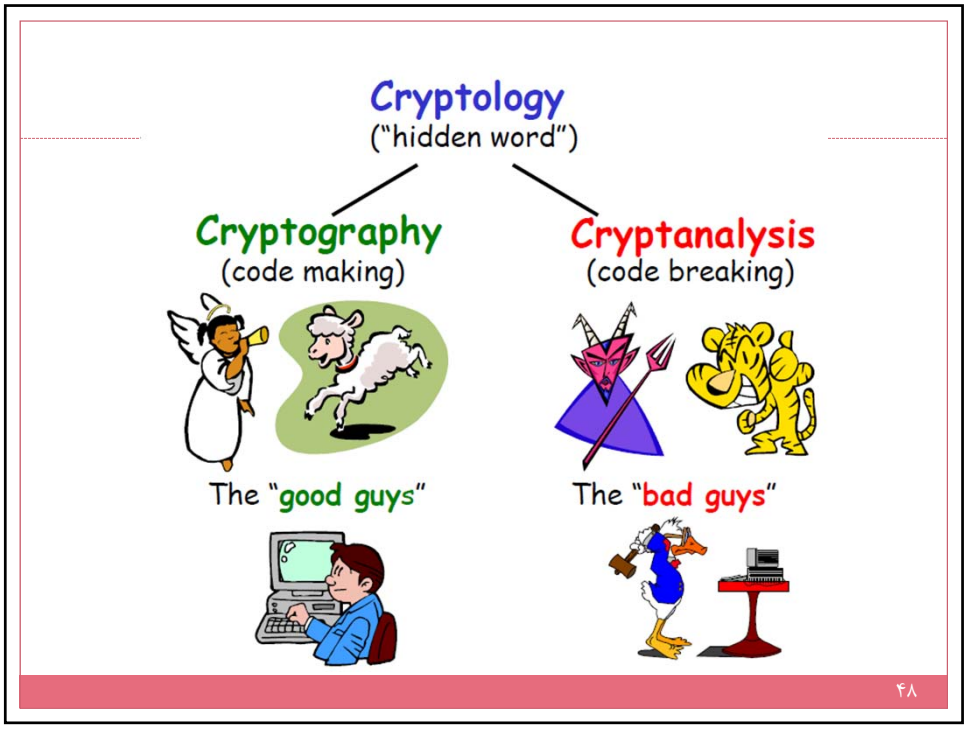
- رمزنگاری (Cryptography): علم و مطالعه روش‌های مختلف مبادله اطلاعات امن
- متن اصلی (Plaintext=cleartext): پیام یا متنی که می‌بایست پس از رمز شدن برای گیرنده خاصی ارسال شود
- متن رمزشده (Ciphertext=Cryptogram): متن رمز شده که توسط یک کانال ناامن ارسال می‌گردد
- عمل رمزگذاری (Encipherment=Encryption): فرآیند تبدیل متن اصلی به متن رمزشده
- الگوریتم (Algorithm): روشی که رمزکننده (Encipherer) برای رمز کردن متن اصلی بکار می‌برد
- کلید (Key): الگوریتم عموماً متکی به یک کلید است که می‌بایستی برای دریافت کننده متن رمز شده معلوم باشد و سایرین از آن اطلاعی نداشته باشند

۴۶

تعاریف اساسی

- عمل رمزگشایی (Deciphering=Decryption): عمل استخراج متن اصلی از متن رمز شده توسط گیرنده و با استفاده از کلید
- کد (Code): نحوه ارسالی است که به کلید خاصی بستگی ندارد و فقط به کتاب کد (Codebook) وابسته است. یعنی فقط یک کلید دارد. بنابراین کد را به صورت سیستمی که به کلید وابسته نیست تعریف می‌کنیم
- رمزشکن (Cryptanalyst): کسی که مجوز فهمیدن پیام را ندارد ولی در جستجوی آن است
- رمزشکنی (Cryptanalysis): دانش و مطالعه روش‌های مختلف بدست آوردن پیام توسط رمزشکن
- رمزشناسی (Cryptology): دانش رمزنگاری و رمزشکنی را کلاً رمزشناسی نامند
- سیستم شکست‌پذیر (Breakable): سیستم شکست‌پذیر است هرگاه امکان دست‌یابی به کلید از روی متن رمزشده و یا از روی متن رمزشده و متن اصلی باشد

۴۷



انواع حمله‌ها برای رمزشکنی (از نظر اطلاعات رمزشکن)

1. حمله بر اساس فقط متن رمزشده (Ciphertext Only Attack)
   - اطلاعات: الگوریتم رمزنگاری + متن رمزشده
   - حمله نوع اول
2. حمله بر اساس چند متن اصلی معلوم (Known Plaintext Attack)
   - اطلاعات: الگوریتم رمزنگاری + متن رمزشده + یک یا چند متن اصلی و متون رمزشده متناظر
   - هدف: یافتن کلید
   - حمله نوع دوم
3. حمله متن اصلی منتخب (Chosen Plaintext Attack)
   - اطلاعات: الگوریتم رمزنگاری + متن رمزشده + هر متن اصلی منتخب و متون رمزشده متناظر
   - هدف: یافتن کلید
   - حمله نوع سوم

۴۹

انواع حمله‌ها برای رمزشکنی (ادامه)

4. حمله متن رمز منتخب (Chosen Ciphertext Attack)
   - اطلاعات: الگوریتم رمزنگاری + متن رمزشده + هر متن رمزشده منتخب و متون اصلی رمزگشایی شده متناظر
   - هدف: یافتن کلید
   - حمله نوع چهارم
   - خاص سیستم‌های کلید همگانی
5. حمله متن منتخب (Chosen Text Attack)
   - اطلاعات: الگوریتم رمزنگاری + متن رمزشده + هر متن اصلی منتخب و متون رمزشده متناظر + هر متن رمزشده منتخب و متون اصلی رمزگشایی شده متناظر
   - هدف: یافتن کلید

۵۰

امنیت در سیستم‌های رمزنگاری

1. امنیت بدون شرط (unconditional security):
   - مستقل از امکانات نامحدود رمزشکن، سیستم امن باشد
   - سیستم ورنام (Vernam) = سیستم One time pad
2. امنیت محاسباتی (computational security):
   - رمزشکنی عملاً و از نظر محاسباتی پیچیده و طولانی باشد
   - مانند رمز RSA: امنیت محاسباتی مبتنی بر تجزیه اعداد اول

- فاصله قابل شکست (unicity distance): حداقل طول متنی که در حمله نوع اول لازم است
  - اولین بار توسط شانون
- C.E. Shannon, “Communication Theory of Secrecy Systems,” *Bell System Tech. J., vol. 28, pp. 656-715, Oct., 1949.*

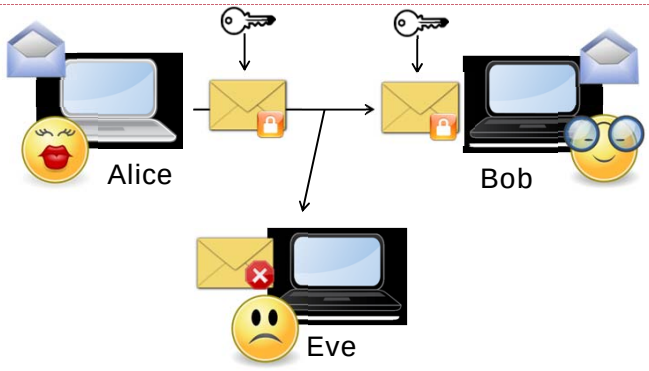
۵۱

معیارهای پنج‌گانه ارزیابی شانون

1. میزان ایمنی سیستم: افزایش N_0
2. اندازه کلید: تا اندازه ممکن کوچک ← مدیریت توزیع و نگهداری کلید
3. پیچیدگی عملیات رمزگذاری و رمزگشایی: تا اندازه ممکن ساده باشند
4. انتشار خطا: جلوگیری
5. بسط یا گسترش پیام: منجر به افزایش ریت ارسال
   - جلوگیری

۵۲

Encryption – رمزنگاری



- Kerckhoffs's principle
  The enemy knows the system
- The cryptographic secret or private keys must be kept secret

۵۳

پارامترهای یک سیستم رمزنگاری

1. فضای پیام (متن) اصلی (plaintext message space): $\forall M \in \mathcal{M}$
2. فضای پیام (متن) رمزشده (ciphertext message space): $\forall C \in \mathcal{C}$
3. فضای کلید: $\forall K \in \mathcal{K}$
4. مجموعه تبدیلات رمزگذاری (Enciphering transformation):

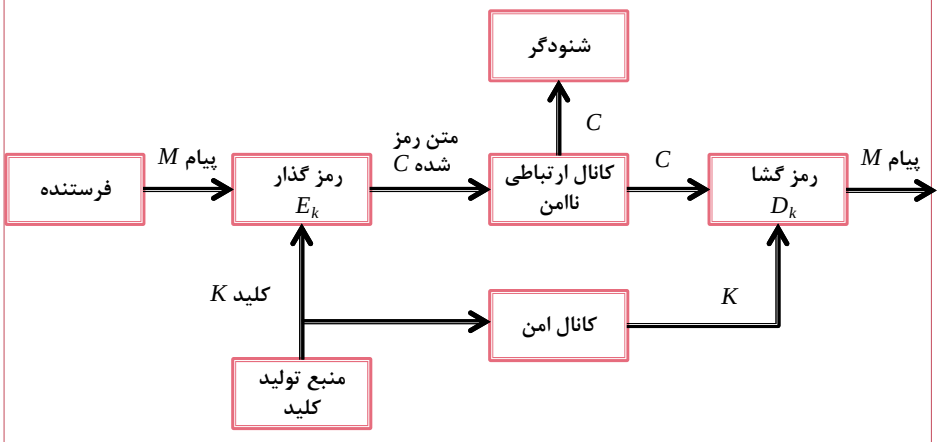
$$E_K : \mathcal{M} \to \mathcal{C} \quad , \quad \forall K \in \mathcal{K}$$

5. مجموعه تبدیلات رمزگشایی (Deciphering transformation):

$$D_K : \mathcal{C} \to \mathcal{M} \quad , \quad \forall K \in \mathcal{K}$$

۵۴

رمزنگاری به منظور محرمانگی (Confidentiality)
رمز متقارن



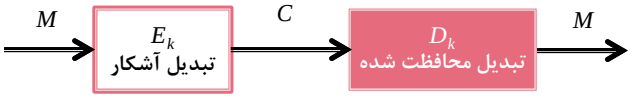
۵۵

شرایط لازم برای محرمانگی پیام

- شنودگر نتواند بر اساس متن رمزشده، متن اصلی را بدست بیاورد:

1. بدست آوردن تبدیل رمزگشایی D_K بر اساس متن رمزشده C و حتی با معلوم بودن متن اصلی متناظر با آن از نظر محاسباتی برای شنودگر غیرممکن باشد. یعنی، نتواند به صورت سیستماتیک D_K را و در نتیجه M را بیابد.
2. بدست آوردن متن اصلی M از متن رمزشده C از نظر محاسباتی برای شنودگر غیرممکن باشد. یعنی، نتواند بدون داشتن تبدیل رمزگشایی D_K به متن اصلی M دست بیابد.

- D_K محرمانه
- نیازی به محرمانه بودن E_K نیست مشروط بر این که E_K اطلاعاتی از D_K ندهد.

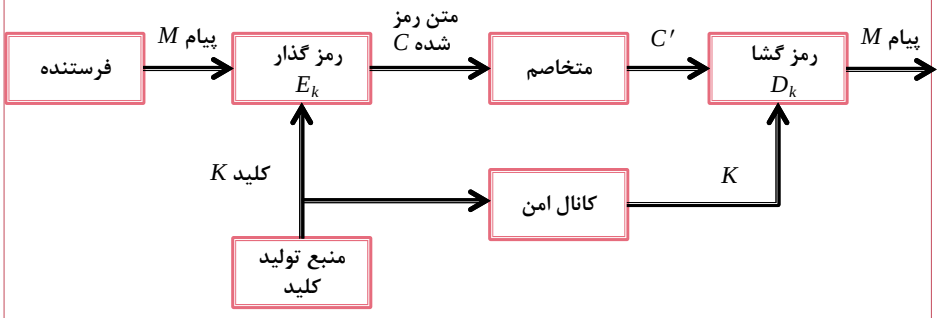


۵۶

رمزنگاری به منظور احراز اصالت (Authentication) پیام

(یکپارچگی (Integrity) پیام)

رمز متقارن



۵۷

شرایط لازم برای اصالت یا اعتبار پیام (Authenticity requirements)

- متخاصم نتواند یک متن جعلی C' را به جای متن معتبر C قرار دهد. یعنی، در این صورت می‌بایست متن جعلی کشف شود:

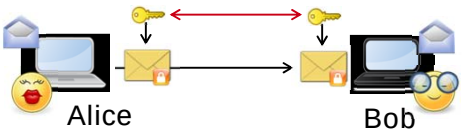
1. بدست آوردن تبدیل رمزگذاری E_K بر اساس متن رمزشده C و حتی با معلوم بودن متن اصلی M متناظر با آن از نظر محاسباتی برای متخاصم غیرممکن باشد. یعنی، نتواند متن جعلی M' را برای گیرنده به صورت $C' = E_K(M')$ (که C' ارسال کند.
2. بدست آوردن سیستماتیک C' به طوریکه $D_K(C')$ یک متن اصلی M باشد، از نظر محاسباتی برای متخاصم غیرممکن باشد. یعنی، نتواند متنی مثل C' را بیابد که به یک متن معتبر رمزگشایی شود (بدون اطلاع از تبدیل رمزگذاری E_K)

- E_K محرمانه
- نیازی به محرمانه بودن D_K نیست مشروط بر این که D_K اطلاعاتی از E_K ندهد.

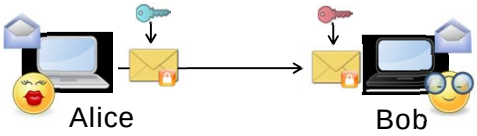
۵۸

انواع رمزنگاری

- رمزنگاری متقارن (کلید مخفی)
  - Symmetric=One Key
  - Classic crypto systems, conventional systems



- رمزنگاری نامتقارن (کلید همگانی)
  - Asymmetric=Two Key
  - Public-Key Cryptography



۵۹

تقسیم‌بندی سیستم‌ها از نظر تبدیلات رمزگذاری و رمزگشایی

- سیستم متقارن یا تک کلیدی (Symmetric=One Key)
  - کلیدهای رمزگذاری و رمزگشایی یکسان یا به راحتی از روی یکدیگر قابل محاسبه
  - رابطه ساده میان تبدیلات رمزگذاری و رمزگشایی
  - محرمانگی و اعتبار توام
  - سیستم‌های کلاسیک یا متداول
- سیستم نامتقارن یا دو کلیدی (Asymmetric=Two Key)
  - رابطه مشکل (یک طرفه) میان تبدیلات رمزگذاری و رمزگشایی
  - کلیدهای رمزگذاری و رمزگشایی متفاوت
  - یکی از کلیدها می‌تواند آشکار (همگانی) باشد
  - محرمانگی و اعتبار به طور جداگانه نیز قابل بررسی
  - سیستم‌های مدرن: سیستم‌های کلید همگانی

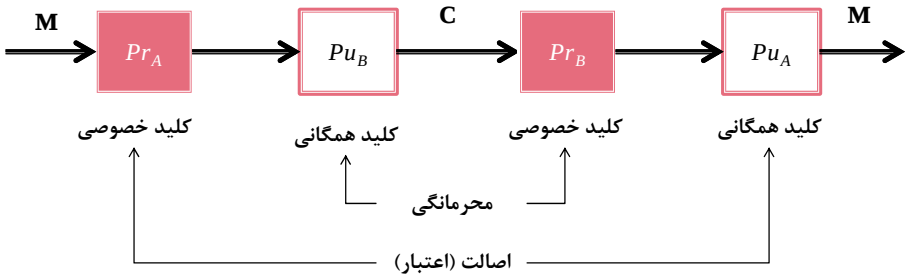
۶۰

سیستم‌های کلید همگانی (Public Key Systems)

- معرفی در سال ۱۹۷۶ توسط دیفی و هلمن (Diffie & Hellman)
- معرفی مستقلاً توسط مرکل (Merkle)
- هر کاربر دارای دو کلید است: مثلاً کاربر A
  - یک کلید همگانی (public): همه می‌دانند Pu_A
  - یک کلید خصوصی (private) مخفی: تنها نزد خود کاربر Pr_A
  - توابع یک‌طرفه:
    - محاسبه Pr_A از روی Pu_A از نظر محاسباتی غیرممکن
    - محاسبه Pu_A از روی Pr_A ساده
- محرمانگی و اصالت (اعتبار) به طور جداگانه

۶۱

محرمانگی و اصالت (اعتبار) توام در سیستم‌های کلید همگانی



- مهم‌ترین مزیت سیستم‌های کلید همگانی
  - نیازی به ارسال کلید از طریق یک کانال امن نیست
  - از این لحاظ برتری عمده بر سیستم‌های کلاسیک

۶۲

امضای دیجیتال
Digital Signature

اصالت یا اعتبار اطلاعات دریافتی: ارسال پیام امضا شده *M* توسط منبع A به منبع B

1. اصالت امضای فرستنده (Sender authenticity)
   - گیرنده مطمئن باشد که پیام از منبع فرستنده است
   - B باید مطمئن باشد که پیام متعلق به A است ← تایید اصالت امضای A
2. اصالت پیام (Message (data) authenticity)
   - امکان تغییر پیام توسط دیگری و یا حتی گیرنده نباشد
   - جعل امضای A برای هر فرد و از جمله خود B غیرممکن باشد. یعنی هیچ منبع دیگری نتواند پیامی را به نام منبع A برای B ارسال کند و حتی B هم نتواند پیامی غیر از M را به عنوان پیامی از جانب A ارائه دهد
3. انکارناپذیری (منبع)
   - فرستنده بعداً نتواند ارسال پیام را انکار کند
   - هر مرجعی با بررسی پیام دریافتی بتواند منبع ارسال آن یعنی A را مشخص کند

۶۳

امضای دیجیتال
سیستم‌های کلید همگانی

- کلید خصوصی Pr_A: نقش امضا
- منبع A پیام M را با کلید خصوصی Pr_A امضا کرده و برای B می‌فرستد
- متن رمزشده $c= Pr_A(M)$ توسط B دریافت می‌شود
- B با استفاده از کلید همگانی A یعنی Pu_A، اصالت (اعتبار) پیام و تعلق آن به A را کشف می‌کند
- $Pr_A(M)$: پیام امضا شده A
- $Pu_A(c)= Pu_A(Pr_A(M))=M$ توسط B کشف می‌شود
- در صورت بروز اختلاف، مرجع سوم می‌تواند ادعای B مبنی بر ارسال پیام توسط A را با بررسی متن امضا شده یعنی $Pr_A(M)$، بررسی کند
  - چون $Pu_A(c)= M$ است و هیچ منبعی جز A اطلاع از کلید Pr_A ندارد، پیام M متعلق به A است و نمی‌تواند ارسال آن را انکار نماید

۶۴

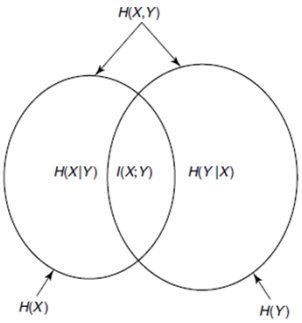
امضای دیجیتال
سیستم متقارن

- Merkle
- منبع سوم مورد اعتماد (S) : کلیدهای رمزگذاری و رمزگشایی A و B را می‌داند
- ارسال پیام امضا شده M توسط منبع A به منبع B
- منبع A پیام رمزشده $c= D_A(M)$ برای B می‌فرستد
- برای بررسی اصالت، B پیام رمزشده c را برای S می‌فرستد
- S صحت آن را با محاسبه $E_A(c)=M$ مشخص کرده و پیام M را با استفاده از کلید محرمانه B برای B می‌فرستد
- B پیام M را رمزگشایی می‌کند

۶۵

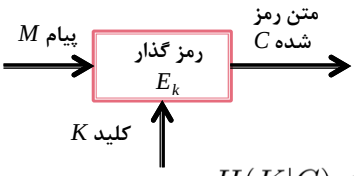
مروری بر نظریه اطلاعات (Information Theory)

- مقاله ۱۹۴۹ شانون: نظریه رمزنگاری بر اساس نظریه اطلاعات
- آنتروپی یک منبع اطلاعات گسسته و بدون حافظه
- اطلاعات متقابل (Mutual Information)



۶۶

ارزیابی کیفی سیستم رمزنگاری



- هدف مهاجم: کلید
  - متن رمزشده حداقل اطلاعات را در مورد کلید بدهد
  - H(K|C) حداکثر شود

$$H(K|C) \leq H(K) \leq \log |\mathcal{K}|$$

اندازه الفبای کلید

- دنباله کلید مستقل از دنباله متن رمزشده باشد
- کلیدها با احتمال مساوی اتفاق بیفتند
- تعداد کلیدها افزایش یابد
  - با ارزیابی عملی شانون جهت مدیریت کلید مغایرت دارد

۶۷

افزونگی یک زبان (Redundancy of a language)

- نرخ واقعی زبان (actual rate of a language)
  - متوسط اطلاعات موجود در هر سمبل
  - انگلیسی: r=1-1.5 بیت بر سمبل
  - فارسی: r=1.5 بیت بر سمبل

$$r = \lim_{n\to\infty} \frac{H(X)}{N}$$

- نرخ مطلق زبان (absolute rate of a language)
  - نرخ اطلاعات در هر سمبل وقتی سمبل‌ها به صورت مستقل و با احتمال مساوی تولید شوند
  - L=تعداد سمبل‌های زبان مورد نظر (تعداد حروف الفبا)
  - انگلیسی: $R = \log 26 = 4.7\,\text{bit/sym}$
  - فارسی: $R = \log 32 = 5\,\text{bit/sym}$

$$R = \log L$$

- افزونگی: تفاوت نرخ واقعی و مطلق $D = R - r$

ساختار زبان (فرکانس حروف)

- توزیع فرکانس نسبی حروف (تک حرفی):
  - انگلیسی: حروف فرکانس بالا: RATE - حروف فرکانس پایین: XYZ
  - فارسی: حروف فرکانس بالا: ا ی رد - حروف فرکانس پایین: ژ ث

حرف	فرکانس
ا	٪۱۴.۵
ی	٪۹
ر	٪۸.۵
د	٪۷.۴
ث	٪۰.۰۹
ژ	٪۰.۰۷

حرف	فرکانس
E	٪۱۳
T	٪۹
A	٪۷.۵
X	٪۰.۱۵
Z	٪۰.۰۷۴

ساختار زبان (فرکانس حروف)

- توزیع فرکانس نسبی دوحرفی‌ها (Digram):

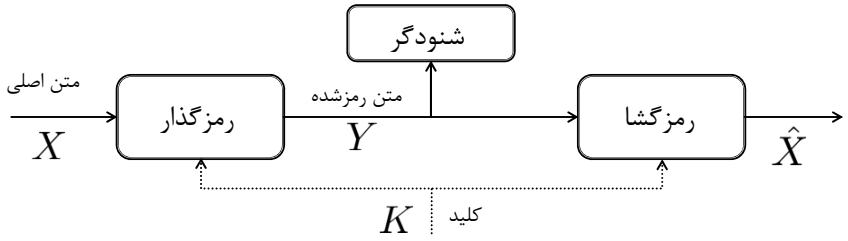
حرف	فرکانس
TH	٪۳.۰۱
ER	٪۱.۸۶
AN	٪۱.۴۲
EN	٪۱.۱۴
VP	٪۰.۰۰۱
ZB	۰

حرف	فرکانس
ان	٪۲.۴۱
ای	٪۱.۹۶
چب	۰

- توزیع فرکانس نسبی سه حرفی‌ها (Trigram):
  - برخی سه حرفی‌ها مانند THE، ING و AND خیلی بیشتر از سایر سه حرفی‌ها تکرار می‌شوند

۷۰

مدل رمزنگاری شانون



- عدم ابهام در رمزگشایی:

$$X = \hat{X} \mapsto H(X|Y,K) = 0$$

- سیستم امن کامل (Perfectly secure):
  - ابهام کلید بیشتر از ابهام متن اصلی
  - سیستم ورنام (one-time pad)

$$I(X;Y) = 0 \iff X \perp\!\!\!\perp Y$$
$$H(K) \geq H(X)$$
$$Y = X \oplus K$$

۷۱

فاصله قابل شکست (unicity distance)

- حداقل طول متن رمزشده که در حمله نوع اول لازم است تا رمز شکسته شود
- کوچک‌ترین nای که با دریافت n سمبل متن رمز شده ابهام کلید تقریباً برابر صفر شود

$$H(K|Y_1,\ldots,Y_n) \approx 0$$

- محاسبه اغلب مشکل و غیرعملی
- هلمن – شانون
  - رمزهای تصادفی (Random cipher)

$$N_0 = \frac{H(K)}{D}$$

۷۲

دو ساختار پیشنهادی شانون برای کاهش اثرات حمله‌های آماری

1. **پراکنش (Diffusion)**: تبدیلاتی را شامل می‌شود که خواص آماری متن اصلی را در طول متن رمزشده پراکنده می‌کند
   - هر سمبل متن اصلی روی تعداد زیادی از سمبل‌های متن رمزشده تاثیر گذارد یا به طور معادل هر سمبل متن رمزشده از تعداد زیادی از سمبل‌های متن اصلی تاثیر پذیرد
   - رابطه بین متن اصلی و متن رمز شده پیچیده می‌شود
   - تغییر فرکانس نسبی
   - جایگشت (permutation) + اعمال توابع
2. **آشفته‌سازی (Confusion)**: رابطه بین کلید و متن رمزشده پیچیده شود
   - الگوریتم جانشینی (substitution) پیچیده

- **اساس طراحی رمزهای قالبی مدرن**

۷۳

نظریه اعداد (Number Theory)

- هم‌نهشت‌ها (congruence) و حساب پیمانه‌ای (modular arithmetic)
- محاسبه معکوس (ضربی) اعداد در فضای mod n
  - تابع اولر
  - قضیه اولر – فرمت
- حل معادلات هم‌نهشتی
- قضیه باقیمانده چینی (The Chinese Remainder Theorem)
- میدان گالوا (Galois field)
  - میدان‌های متناهی GF(p)

۷۴