UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
UNIVERSITY OF SZEGED
Department of Software Engineering

Hálózati Modellek és Protokollok

Dr. Bilicki Vilmos
Szoftverfejlesztés Tanszék

A fóliákhoz felhasznált anyagok:
Computer Networking: A Top Down Approach , 7th edition Jim Kurose, Keith Ross
Pearson/Addison Wesley, April 2016

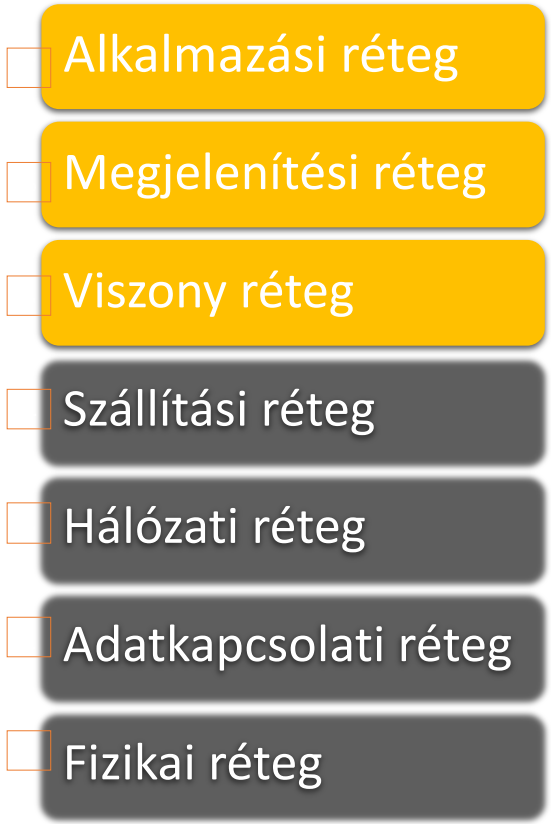
Áttekintés

- Bevezetés a hálózati biztonságba
  - CIA modell és alapvető biztonsági koncepciók
  - Fenyegetettségi környezet és támadási vektorok
- Kriptográfiai alapok
  - Alapvető terminológiák és folyamatok
  - Kerckhoffs elve és Shannon maximája
  - Kulcsfontosságú biztonsági elvek: Legkisebb jogosultság és Mélységi védelem
- Szimmetrikus titkosítási rendszerek
  - Elvek, példák és műveletek
  - Előnyök, korlátok és kulcskezelés
- Aszimmetrikus titkosítási rendszerek
  - Nyilvános és privát kulcs koncepciók
  - RSA és egyéb algoritmusok
  - Alkalmazások és összehasonlító elemzés
- Kivonat (Hash) függvények és digitális aláírások
  - Alapkoncepciók és biztonsági alkalmazások
  - Digitális aláírási folyamatok és integritás
- Nyilvános kulcsú infrastruktúra (PKI)
  - Komponensek és műveletek
  - Hitelesítésszolgáltatók szerepe
  - Digitális tanúsítványok és SSL/TLS bevezetés
- Következtetés és jövőbeli perspektívák
  - Kulcsfontosságú hálózati biztonsági koncepciók összefoglalása
  - Kiberbiztonság új kihívásai

Rétegzés: Egy Hatékony Megközelítés

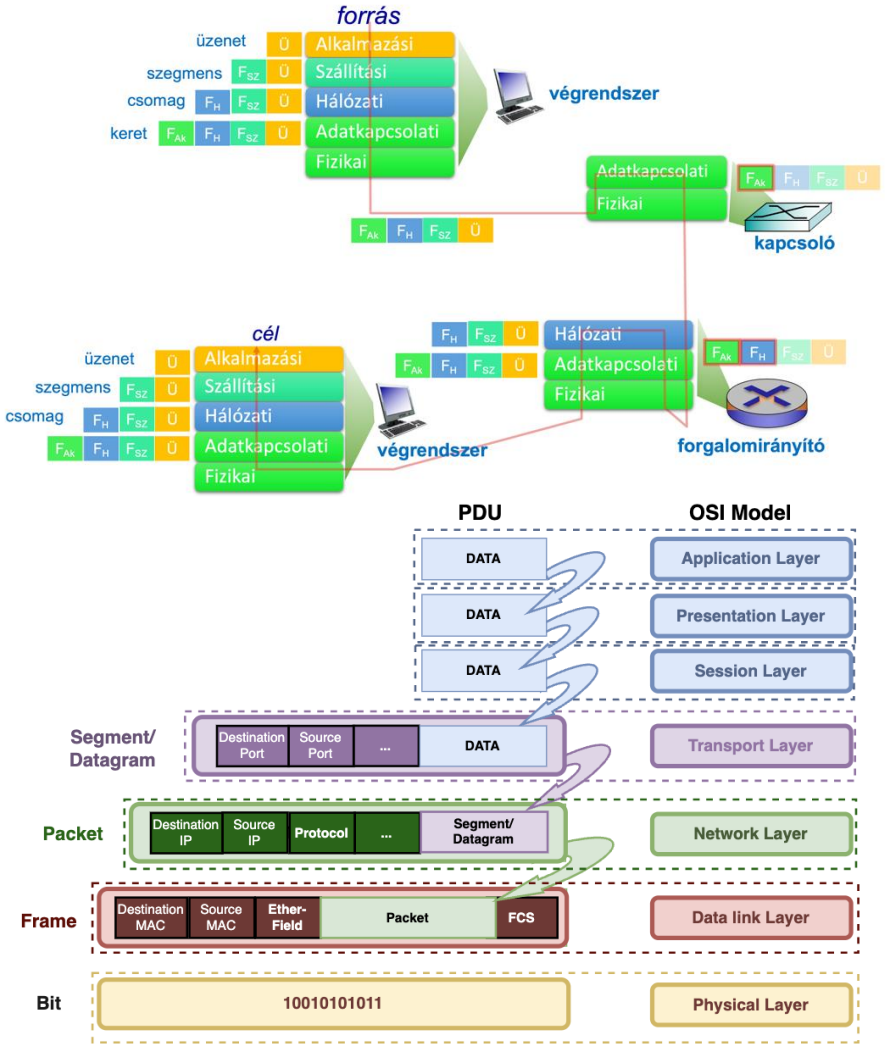
- Funkcionalitás logikai felosztása
  - Jól definiált felelősségi körök
  - Komplexitás kezelése
- Absztrakciós szintek kialakítása
  - Részletek elrejtése
  - Magasabb szintű műveletek lehetővé tétele
- Szabványosított interfészek rétegek között
  - Világos kommunikációs szabályok
  - Modulok cserélhetősége

OSI rétegek



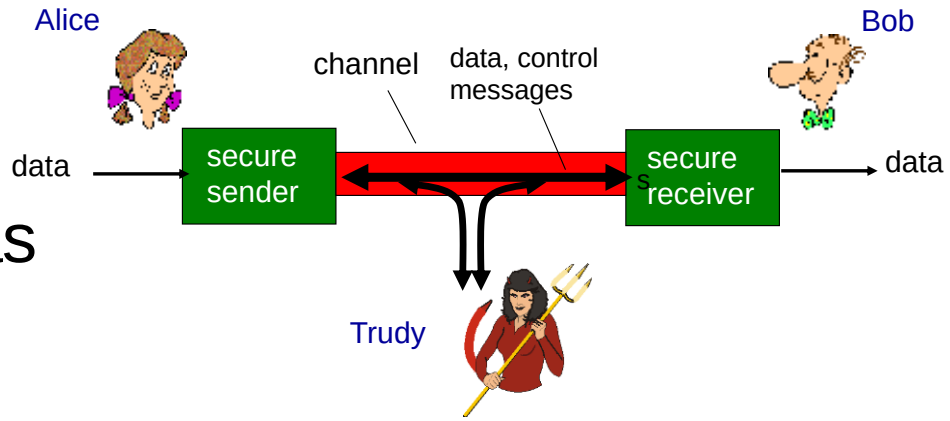
PDU: A Hálózat Adatstruktúrái

- PDU (Protocol Data Unit) definíció
  - A hálózati kommunikáció alapegysége
  - Rétegenként változó elnevezés és struktúra
- PDU komponensek
  - Fejléc (Header): Vezérlő információk
  - Adat (Payload): Tényleges tartalom
  - Lábléc (Trailer): Opcionális, pl. hibaellenőrzés
- PDU típusok rétegenként
  - Alkalmazási réteg: Üzenet
  - Szállítási réteg: Szegmens (TCP) / Datagram (UDP)
  - Hálózati réteg: Csomag
  - Adatkapcsolati réteg: Keret



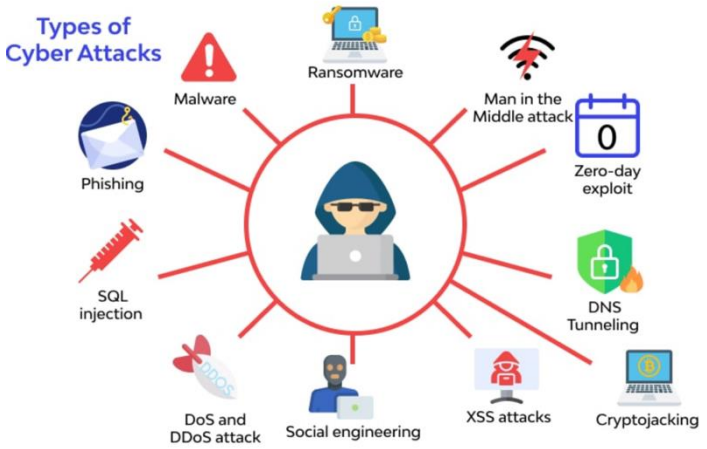
Hálózati biztonság alapjai: A CIA modell

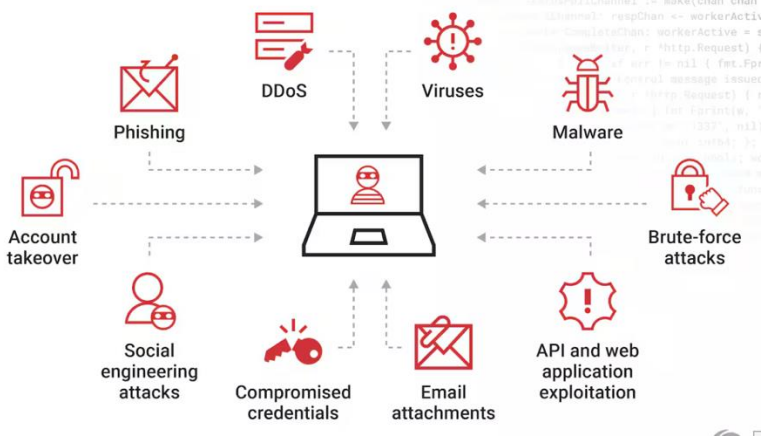
- Hálózati biztonság definíciója
- Hálózati biztonság fontossága
- A CIA modell:
  - Bizalmasság (Confidentiality)
  - Sértetlenség (Integrity)
  - Rendelkezésre állás (Availability)



Gyakori kiberfenyegetések és támadási vektorok

- Főbb kiberfenyegetések:
  - Malware (rosszindulatú szoftverek)
  - Adathalászat (phishing)
  - Szolgáltatásmegtagadás (Denial of Service, DoS)
  - Közbeékelődéses támadás (Man-in-the-Middle, MitM)
- Gyakori támadási vektorok:
  - Kompromittált hitelesítő adatok
  - Szoftver sebezhetőségek
  - Social engineering (Közösségi manipuláció)
  - Belső fenyegetések



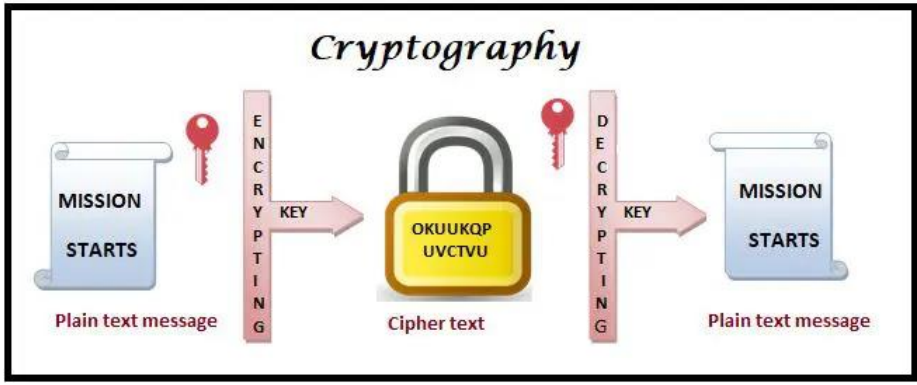


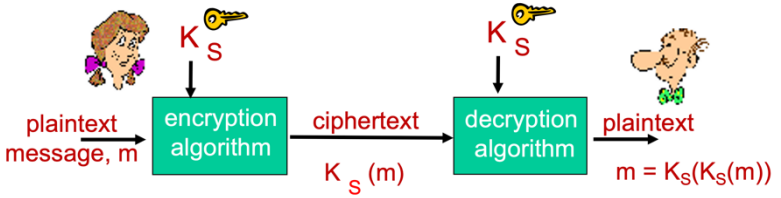
Áttekintés

- Bevezetés a hálózati biztonságba
  - CIA modell és alapvető biztonsági koncepciók
  - Fenyegetettségi környezet és támadási vektorok
- Kriptográfiai alapok
  - Alapvető terminológiák és folyamatok
  - Kerckhoffs elve és Shannon maximája
  - Kulcsfontosságú biztonsági elvek: Legkisebb jogosultság és Mélységi védelem
- Szimmetrikus titkosítási rendszerek
  - Elvek, példák és műveletek
  - Előnyök, korlátok és kulcskezelés
- Aszimmetrikus titkosítási rendszerek
  - Nyilvános és privát kulcs koncepciók
  - RSA és egyéb algoritmusok
  - Alkalmazások és összehasonlító elemzés
- Kivonat (Hash) függvények és digitális aláírások
  - Alapkoncepciók és biztonsági alkalmazások
  - Digitális aláírási folyamatok és integritás
- Nyilvános kulcsú infrastruktúra (PKI)
  - Komponensek és műveletek
  - Hitelesítésszolgáltatók szerepe
  - Digitális tanúsítványok és SSL/TLS bevezetés
- Következtetés és jövőbeli perspektívák
  - Kulcsfontosságú hálózati biztonsági koncepciók összefoglalása
- Kiberbiztonság új kihívásai

Kriptográfia alapjai: Fogalmak és folyamatok

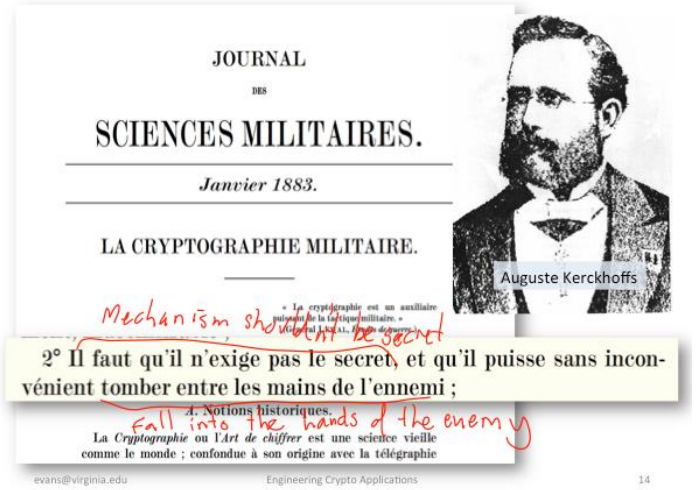
- Kulcsfontosságú kriptográfiai kifejezések:
  - Nyílt szöveg (Plaintext)
  - Titkosított szöveg (Ciphertext)
  - Titkosítási kulcs (Encryption Key)
  - Visszafejtési kulcs (Decryption Key)
- Titkosítási folyamat
- Visszafejtési folyamat
- Kriptográfiai algoritmusok típusai:
  - Szimmetrikus
  - Aszimmetrikus

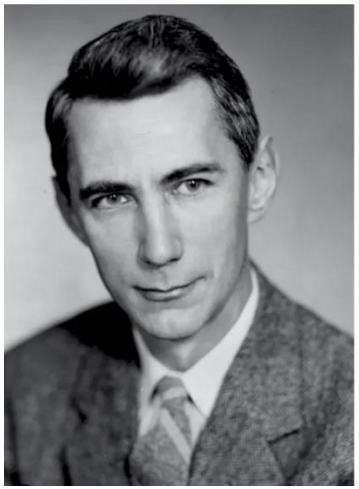




Alapvető kriptográfiai elvek: Kerckhoff és Shannon

- Kerckhoff elve:
  - A rendszer biztonsága a kulcs titkosságán alapul, nem az algoritmus titkosságán
  - Fontossága a modern kriptográfiában
- Shannon maximája:
  - "Az ellenség ismeri a rendszert"
  - Feltételezi, hogy a támadó mindent tud, kivéve a kulcsot
- Következmények a kriptográfiai rendszerek tervezésére:
  - Nyílt algoritmusok, titkos kulcsok
  - Szakértői áttekintés és nyilvános vizsgálat

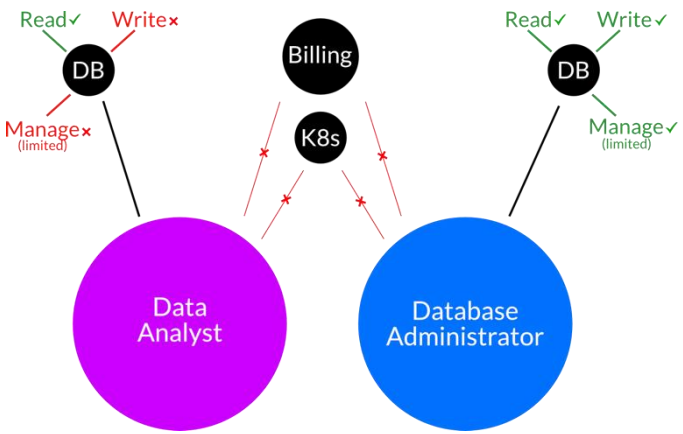

JOURNAL
DES
SCIENCES MILITAIRES.
Janvier 1883.
LA CRYPTOGRAPHIE MILITAIRE.
Auguste Kerckhoffs
Mechanism should not be secret
2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;
fall into the hands of the enemy
1. Notions historiques.
La *Cryptographie* ou *L'Art de chiffrer* est une science vieille comme le monde ; confondue à son origine avec la télégraphie
evans@virginia.edu Engineering Crypto Applications 14

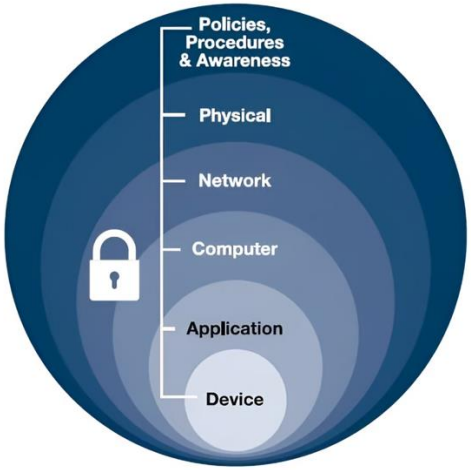



Communication Theory of Secrecy Systems*
By C. E. SHANNON
1. Introduction and Summary
THE problems of cryptography and secrecy systems furnish an interesting application of communication theory.[1] In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography.[2] There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.
The treatment is limited in certain ways. First, there are three general types of secrecy system: (1) concealment systems, including such methods as invisible ink, concealing a message in an innocent text, or in a fake covering cryptogram, or other methods in which the existence of the message is concealed from the enemy; (2) privacy systems, for example speech inversion, in which special equipment is required to recover the message; (3) "true" secrecy systems where the meaning of the message is concealed by cipher, code, etc., although its existence is not hidden, and the enemy is assumed to have any special equipment necessary to intercept and record the transmitted signal. We consider only the third type—concealment systems are primarily a psychological problem, and privacy systems a technological one.
Secondly, the treatment is limited to the case of discrete information, where the message to be enciphered consists of a sequence of discrete symbols, each chosen from a finite set. These symbols may be letters in a language, words of a language, amplitude levels of a "quantized" speech or video signal, etc., but the main emphasis and thinking has been concerned with the case of letters.
The paper is divided into three parts. The main results will now be briefly summarized. The first part deals with the basic mathematical structure of secrecy systems. As in communication theory a language is considered to
* The material in this paper appeared originally in a confidential report "A Mathematical Theory of Cryptography" dated Sept. 1, 1945, which has now been declassified.
[1] Shannon, C. E., "A Mathematical Theory of Communication," *Bell System Technical Journal*, July 1948, p. 379; Oct. 1948, p. 623.
[2] See, for example, H. F. Gaines, "Elementary Cryptanalysis," or M. Givierge, "Cours de Cryptographie."

Alapvető biztonsági elvek: Legkisebb jogosultság és Mélységi védelem

- Legkisebb jogosultság elve:
  - Definíció és fontosság
  - Megvalósítás rendszerekben és hálózatokban
  - Előnyök és kihívások
- Mélységi védelem:
  - Rétegzett biztonsági megközelítés
  - Többszörös védelmi mechanizmusok
  - Példák a hálózati biztonságban
- Az elvek közötti szinergia
- Alkalmazás a modern kiberbiztonságban





Kriptoanalízis, Kulcserősség

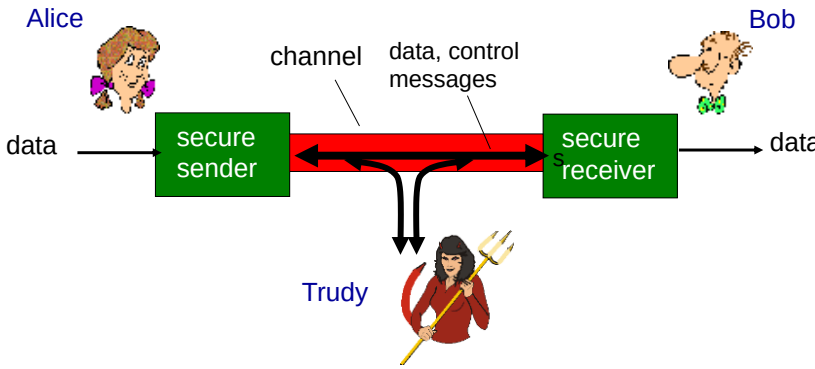
- Gyakori támadások a titkosítás ellen:
  - Brute Force (Nyers erő) támadás
  - Ismert nyílt szöveg (Known-Plaintext) támadás
  - Választott titkosított szöveg (Chosen-Ciphertext) támadás
  - Oldalcsatorna (Side-Channel) támadások
  - Közbeékelődéses (Man-in-the-Middle) támadás
- Kulcshossz és biztonság:
  - A kulcshossz és a támadás ellenállóképesség közötti kapcsolat
  - A Moore-törvény hatása a kriptográfiai biztonságra
  - Ajánlott kulcshosszok különböző algoritmusokhoz

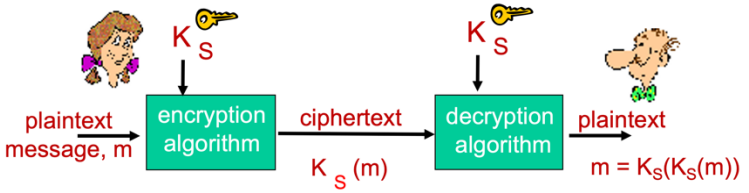
Áttekintés

- Bevezetés a hálózati biztonságba
  - CIA modell és alapvető biztonsági koncepciók
  - Fenyegetettségi környezet és támadási vektorok
- Kriptográfiai alapok
  - Alapvető terminológiák és folyamatok
  - Kerckhoffs elve és Shannon maximája
  - Kulcsfontosságú biztonsági elvek: Legkisebb jogosultság és Mélységi védelem
- Szimmetrikus titkosítási rendszerek
  - Elvek, példák és műveletek
  - Előnyök, korlátok és kulcskezelés
- Aszimmetrikus titkosítási rendszerek
  - Nyilvános és privát kulcs koncepciók
  - RSA és egyéb algoritmusok
  - Alkalmazások és összehasonlító elemzés
- Kivonat (Hash) függvények és digitális aláírások
  - Alapkoncepciók és biztonsági alkalmazások
  - Digitális aláírási folyamatok és integritás
- Nyilvános kulcsú infrastruktúra (PKI)
  - Komponensek és műveletek
  - Hitelesítésszolgáltatók szerepe
  - Digitális tanúsítványok és SSL/TLS bevezetés
- Következtetés és jövőbeli perspektívák
  - Kulcsfontosságú hálózati biztonsági koncepciók összefoglalása
- Kiberbiztonság új kihívásai

Szimmetrikus titkosítás: Elvek és példák

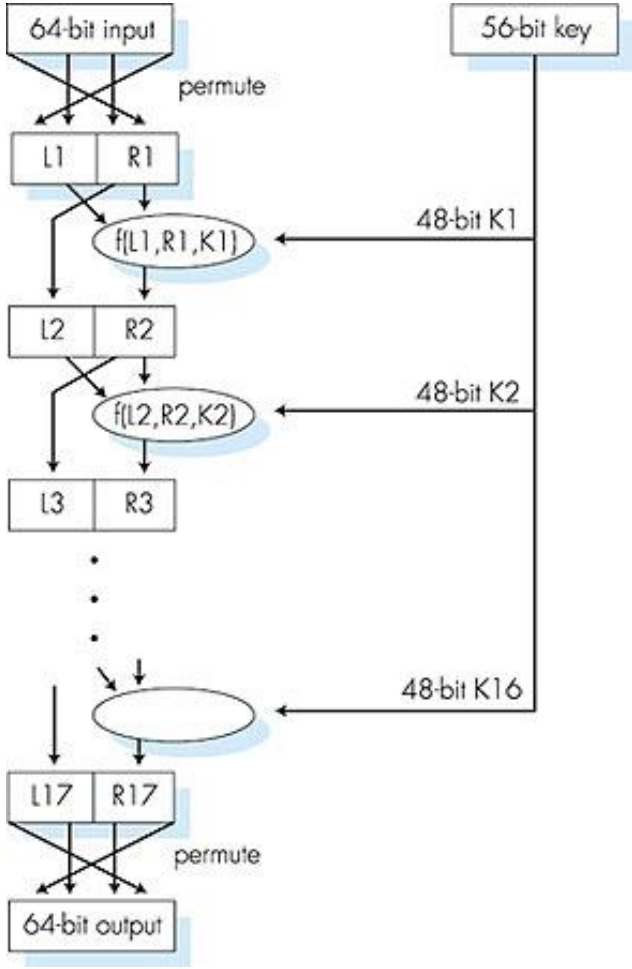
- Szimmetrikus titkosítás definíciója
- Főbb jellemzők:
  - Egyetlen megosztott kulcs
  - Gyors és hatékony
  - Alkalmas nagy adatmennyiségekhez
- Titkosítási/Visszafejtési folyamat
- Gyakori szimmetrikus algoritmusok:
  - AES (Advanced Encryption Standard)
  - DES (Data Encryption Standard)
  - 3DES (Triple DES)
- Blokk titkosítók vs. Folyam titkosítók





Szimmetrikus titkosítás: Előnyök, hátrányok és kulcskezelés

- Szimmetrikus titkosítás előnyei:
  - Sebesség és hatékonyság
  - Erős biztonság megfelelő implementáció esetén
  - Alacsony számítási igény
- Korlátok:
  - Kulcselosztás problémája
  - Skálázhatósági problémák nagy hálózatokban
  - Az inherens hitelesítés hiánya
- Kulcskezelési kihívások:
  - Biztonságos kulcscsere
  - Kulcsok tárolása és védelme
  - Kulcsrotáció és életciklus-kezelés



Szimmetrikus titkosítás: Összefoglalás és valós alkalmazások

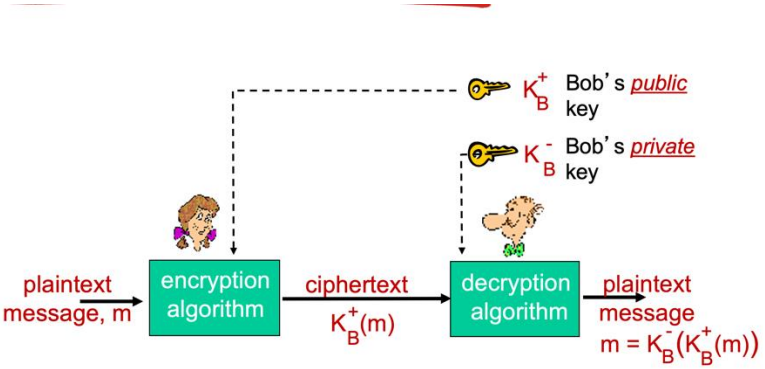
- Kulcspontok összefoglalása:
  - Egyetlen megosztott kulcs
  - Gyors és hatékony
  - Kulcskezelési kihívások
- Gyakori felhasználási esetek:
  - Fájl- és lemeztitkosítás
  - Adatbázis-titkosítás
  - Biztonságos kommunikációs csatornák
- Legjobb gyakorlatok:
  - Erős, szabványosított algoritmusok használata (pl. AES)
  - Megfelelő kulcskezelés implementálása
  - Kombinálás más biztonsági intézkedésekkel

Áttekintés

- Bevezetés a hálózati biztonságba
  - CIA modell és alapvető biztonsági koncepciók
  - Fenyegetettségi környezet és támadási vektorok
- Kriptográfiai alapok
  - Alapvető terminológiák és folyamatok
  - Kerckhoffs elve és Shannon maximája
  - Kulcsfontosságú biztonsági elvek: Legkisebb jogosultság és Mélységi védelem
- Szimmetrikus titkosítási rendszerek
  - Elvek, példák és műveletek
  - Előnyök, korlátok és kulcskezelés
- Aszimmetrikus titkosítási rendszerek
  - Nyilvános és privát kulcs koncepciók
  - RSA és egyéb algoritmusok
  - Alkalmazások és összehasonlító elemzés
- Kivonat (Hash) függvények és digitális aláírások
  - Alapkoncepciók és biztonsági alkalmazások
  - Digitális aláírási folyamatok és integritás
- Nyilvános kulcsú infrastruktúra (PKI)
  - Komponensek és műveletek
  - Hitelesítésszolgáltatók szerepe
  - Digitális tanúsítványok és SSL/TLS bevezetés
- Következtetés és jövőbeli perspektívák
  - Kulcsfontosságú hálózati biztonsági koncepciók összefoglalása
- Kiberbiztonság új kihívásai

Aszimmetrikus titkosítás: Elvek és működés

- Aszimmetrikus titkosítás definíciója
- Főbb jellemzők:
  - Nyilvános és privát kulcspár
  - Számításigényes
  - Megoldja a kulcselosztás problémáját
- Alapvető folyamat:
  - Titkosítás a nyilvános kulccsal
  - Visszafejtés a privát kulccsal
- Nyilvános és privát kulcsok szerepe:
  - Nyilvános kulcs: Szabadon terjeszthető
  - Privát kulcs: Titokban tartandó



Aszimmetrikus titkosítás: Példák, előnyök és korlátok

- Gyakori aszimmetrikus algoritmusok:
  - RSA (Rivest-Shamir-Adleman)
  - ECC (Elliptikus görbe kriptográfia)
  - DSA (Digitális aláírás algoritmus)
- Előnyök:
  - Megoldja a kulcselosztás problémáját
  - Lehetővé teszi a digitális aláírásokat
  - Biztosítja a letagadhatatlanságot
- Korlátok:
  - Lassabb, mint a szimmetrikus titkosítás
  - Hosszabb kulcsokat igényel az egyenértékű biztonsághoz
  - Bizonyos típusú támadásokra érzékeny (pl. közbeékelődéses támadás)
- Alkalmazási területek:
  - Biztonságos kulcscsere
  - Digitális aláírások
  - Biztonságos e-mail (pl. PGP)

Elliptic-Curve Digital Signature Algorithm (ECDSA)

NIST Guidelines for Public Key Sizes for AES			
ECC key size (bits)	RSA key size (bits)	Key size ratio	AES key size (bits)
163	1,024	1:6	
256	3,072	1:12	128
384	7,680	1:20	192
512	15,360	1:30	256

Supplied by NIST to ANSIX9F1

Table 1

Aszimmetrikus titkosítás: Összefoglalás és jövőbeli trendek

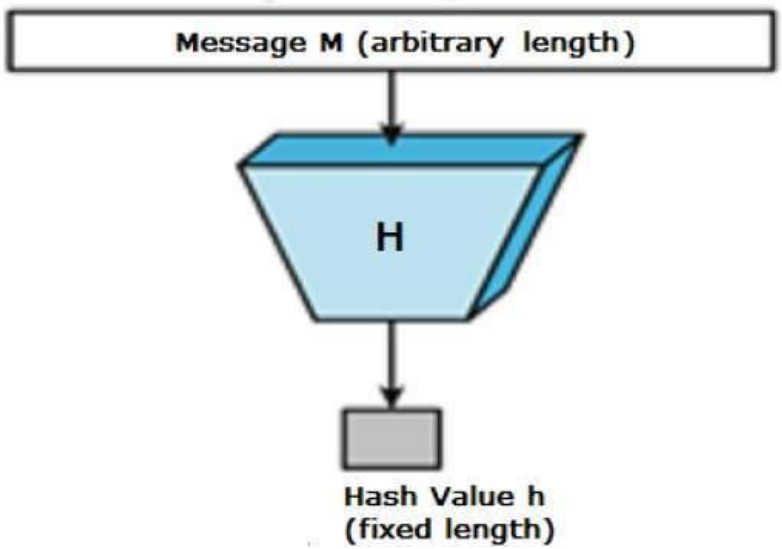
- Kulcspontok összefoglalása:
  - Nyilvános-privát kulcspárok
  - Lassabb, de megoldja a kulcselosztás problémáját
  - Lehetővé teszi a digitális aláírásokat
- Összehasonlítás a szimmetrikus titkosítással
- Hibrid rendszerek:
  - Aszimmetrikus és szimmetrikus titkosítás kombinálása
  - Mindkét módszer előnyeinek kihasználása
- Új trendek:
  - Poszt-kvantum kriptográfia
  - Homomorfikus titkosítás
- Legjobb gyakorlatok az implementálásban

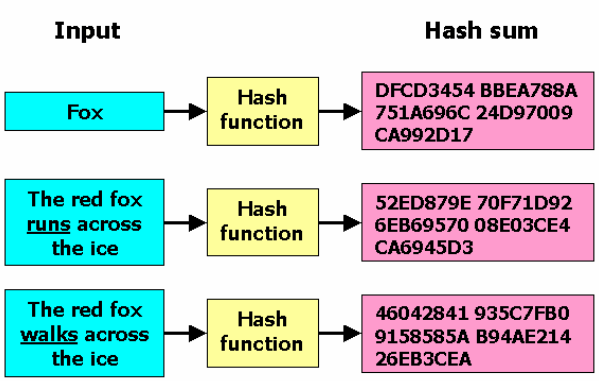
Áttekintés

- Bevezetés a hálózati biztonságba
  - CIA modell és alapvető biztonsági koncepciók
  - Fenyegetettségi környezet és támadási vektorok
- Kriptográfiai alapok
  - Alapvető terminológiák és folyamatok
  - Kerckhoffs elve és Shannon maximája
  - Kulcsfontosságú biztonsági elvek: Legkisebb jogosultság és Mélységi védelem
- Szimmetrikus titkosítási rendszerek
  - Elvek, példák és műveletek
  - Előnyök, korlátok és kulcskezelés
- Aszimmetrikus titkosítási rendszerek
  - Nyilvános és privát kulcs koncepciók
  - RSA és egyéb algoritmusok
  - Alkalmazások és összehasonlító elemzés
- Kivonat (Hash) függvények és digitális aláírások
  - Alapkoncepciók és biztonsági alkalmazások
  - Digitális aláírási folyamatok és integritás
- Nyilvános kulcsú infrastruktúra (PKI)
  - Komponensek és műveletek
  - Hitelesítésszolgáltatók szerepe
  - Digitális tanúsítványok és SSL/TLS bevezetés
- Következtetés és jövőbeli perspektívák
  - Kulcsfontosságú hálózati biztonsági koncepciók összefoglalása
- Kiberbiztonság új kihívásai

Hash függvények: Koncepciók és biztonsági alkalmazások

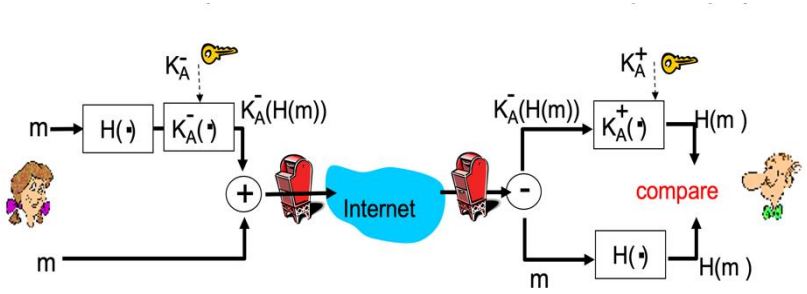
- Hash függvények definíciója
- Kulcsfontosságú tulajdonságok:
  - Rögzített kimeneti méret
  - Egyirányúság (nem megfordítható)
  - Determinisztikus
  - Ütközésállóság
- Gyakori hash függvények:
  - MD5 (elavult)
  - SHA-1 (elavult)
  - SHA-256, SHA-3
- Biztonsági alkalmazások:
  - Adatintegritás
  - Jelszó tárolás
  - Digitális aláírások
  - Proof of Work (Blokklánc)





Digitális aláírások és a hash függvények szerepe

- Digitális aláírás koncepciója
- Digitális aláírás folyamata:
  - Az üzenet hashelése
  - A hash titkosítása a privát kulccsal
  - A titkosított hash csatolása az üzenethez
- Ellenőrzési folyamat:
  - A fogadó fél hasheli a kapott üzenetet
  - Visszafejti az aláírást a küldő nyilvános kulcsával
  - Összehasonlítja a két hasht
- Hash függvények szerepe:
  - Hatékonyság
  - Üzenet integritása
  - Letagadhatatlanság
- Jogi és gyakorlati következmények



Hash függvények és digitális aláírások: Összefoglalás és alkalmazások

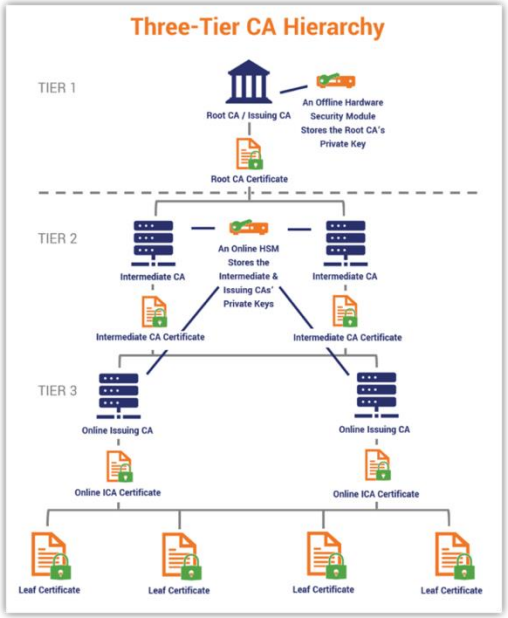
- Kulcspontok összefoglalása:
  - Hash függvények tulajdonságai
  - Digitális aláírás folyamata
- Valós alkalmazások:
  - Kód aláírás
  - E-mail biztonság (S/MIME, PGP)
  - Blokklánc és kriptovaluták
- Biztonsági megfontolások:
  - Ütközésállóság fontossága
  - Privát kulcsok biztonságos tárolása
- Jövőbeli trendek:
  - Poszt-kvantum hash függvények
  - Szabványosítási törekvések

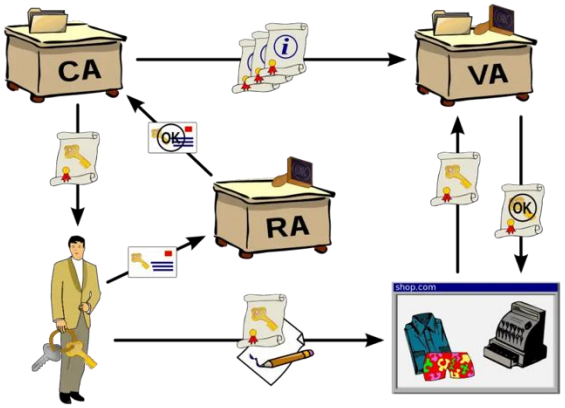
Áttekintés

- Bevezetés a hálózati biztonságba
  - CIA modell és alapvető biztonsági koncepciók
  - Fenyegetettségi környezet és támadási vektorok
- Kriptográfiai alapok
  - Alapvető terminológiák és folyamatok
  - Kerckhoffs elve és Shannon maximája
  - Kulcsfontosságú biztonsági elvek: Legkisebb jogosultság és Mélységi védelem
- Szimmetrikus titkosítási rendszerek
  - Elvek, példák és műveletek
  - Előnyök, korlátok és kulcskezelés
- Aszimmetrikus titkosítási rendszerek
  - Nyilvános és privát kulcs koncepciók
  - RSA és egyéb algoritmusok
  - Alkalmazások és összehasonlító elemzés
- Kivonat (Hash) függvények és digitális aláírások
  - Alapkoncepciók és biztonsági alkalmazások
  - Digitális aláírási folyamatok és integritás
- Nyilvános kulcsú infrastruktúra (PKI)
  - Komponensek és műveletek
  - Hitelesítésszolgáltatók szerepe
  - Digitális tanúsítványok és SSL/TLS bevezetés
- Következtetés és jövőbeli perspektívák
  - Kulcsfontosságú hálózati biztonsági koncepciók összefoglalása
- Kiberbiztonság új kihívásai

Nyilvános kulcsú infrastruktúra (PKI): Koncepciók és komponensek

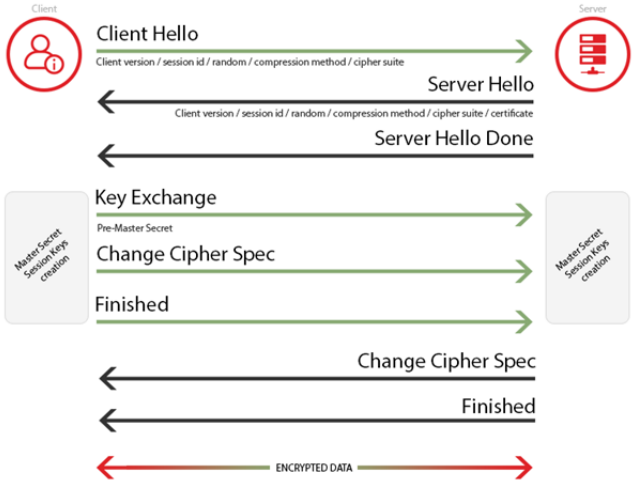
- PKI definíciója
- Főbb komponensek:
  - Hitelesítésszolgáltató (Certificate Authority, CA)
  - Regisztrációs szervezet (Registration Authority, RA)
  - Tanúsítvány-adatbázis
  - Tanúsítványtár
- Digitális tanúsítványok:
  - Szerkezet (X.509 szabvány)
  - Tartalom (nyilvános kulcs, azonosító információk, lejárati dátum)
- Tanúsítvány életciklusa:
  - Kibocsátás
  - Terjesztés
  - Visszavonás
  - Megújítás
- Hitelesítésszolgáltatók (CA-k) szerepe

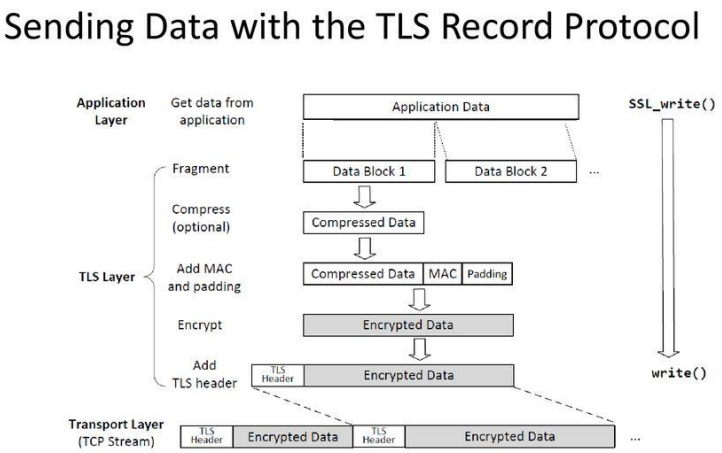




Digitális tanúsítványok és az SSL/TLS bevezetése

- Digitális tanúsítványok fontossága:
  - Identitás ellenőrzés
  - Nyilvános kulcs terjesztés
  - Bizalom kialakítása
- Digitális tanúsítványok gyakori felhasználási területei:
  - Biztonságos böngészés (HTTPS)
  - Biztonságos e-mail (S/MIME)
  - Kód aláírás
- SSL/TLS bevezetés:
  - Secure Sockets Layer (SSL)
  - Transport Layer Security (TLS)
- SSL/TLS kézfogás áttekintése:
  - Kliens üdvözlés
  - Szerver üdvözlés
  - Tanúsítvány csere
  - Kulcscsere
  - Biztonságos kommunikáció





Áttekintés

- Bevezetés a hálózati biztonságba
  - CIA modell és alapvető biztonsági koncepciók
  - Fenyegetettségi környezet és támadási vektorok
- Kriptográfiai alapok
  - Alapvető terminológiák és folyamatok
  - Kerckhoffs elve és Shannon maximája
  - Kulcsfontosságú biztonsági elvek: Legkisebb jogosultság és Mélységi védelem
- Szimmetrikus titkosítási rendszerek
  - Elvek, példák és műveletek
  - Előnyök, korlátok és kulcskezelés
- Aszimmetrikus titkosítási rendszerek
  - Nyilvános és privát kulcs koncepciók
  - RSA és egyéb algoritmusok
  - Alkalmazások és összehasonlító elemzés
- Kivonat (Hash) függvények és digitális aláírások
  - Alapkoncepciók és biztonsági alkalmazások
  - Digitális aláírási folyamatok és integritás
- Nyilvános kulcsú infrastruktúra (PKI)
  - Komponensek és műveletek
  - Hitelesítésszolgáltatók szerepe
  - Digitális tanúsítványok és SSL/TLS bevezetés
- Következtetés és jövőbeli perspektívák
  - Kulcsfontosságú hálózati biztonsági koncepciók összefoglalása
- Kiberbiztonság új kihívásai

Összefoglalás és jövőbeli kihívások

- Kulcsfontosságú pontok:
  - Szimmetrikus vs. Aszimmetrikus titkosítás
  - Hash függvények és digitális aláírások
  - PKI és digitális tanúsítványok
- Új technológiák:
  - Homomorfikus titkosítás
  - Blokklánc a biztonságban
- Jövőbeli kihívások:
  - Poszt-kvantum biztonság
  - IoT biztonság
  - AI és gépi tanulás a kiberbiztonságban
- A folyamatos tanulás fontossága