Investeşte în oameni!
FONDUL SOCIAL EUROPEAN
Programul Operaţional Sectorial Dezvoltarea Resurselor Umane 2007 – 2013
Axa prioritară 1 „Educaţie şi formare profesională în sprijinul creşterii economice şi dezvoltării societăţii bazate pe cunoaştere”
Domeniul major de intervenţie 1.5. „Programe doctorale şi post-doctorale în sprijinul cercetării”
Titlul proiectului: Burse doctorale si postdoctorale pentru cercetare de excelenta
Numărul de identificare al contractului: POSDRU/159/1.5/S/134378
Beneficiar: Universitatea Transilvania din Braşov

CERCETĂRI PRIVIND UTILIZAREA METODELOR STEGANOGRAFICE ȘI CRIPTOGRAFICE ÎN VEDEREA CREȘTERII SECURITĂȚII SISTEMELOR CYBER-FIZICE

Prof.dr.ing. Liviu MICLEA
Prof.dr.ing. Dorian GORGAN
Șef lucrări dr.ing. Anca NICU

CUPRINS

1. INTRODUCERE

INFORMAȚIA ÎNSEAMNĂ PUTERE!

Din dorința de a proteja informația și de a o face accesibilă doar elitelor, primele texte cifrate datează de peste 4000 de ani și provin din Egiptul Antic.

În **Grecia** scrierile cifrate sunt folosite începând cu secolul V î.e.n. În secolul al IV-lea î.e.n. în Grecia se cunoşteau 16 scrieri cifrate. Istoricul grec Polybius (sec II î.e.n.) este inventatorul unui tabel de cifrare pătrat de dimensiune 5x5, ce stă la baza multor sisteme de cifrare utilizate și azi.

În **Roma** antică secretul informaţiilor politice şi militare se făcea utilizând scrierea secretă (vezi cifrul lui Cezar).

În Asia literatura indiană dă o serie de indicii dintre care Artha-sastra (321-300 î.e.n.), Lalita-Vistara şi Kamasutra.

Stenografia, ştiiţa scrierilor secrete insesizabile camuflate în texte în clar, constituie o forma particulară de secretizare.

1. INTRODUCERE

CIFRUL LUI CEZAR

Obținut prin **Tehnica substituției** presupune că literele din textul clar sunt înlocuite de alte litere, sau de numere sau simboluri.[6]

Cifrul lui Cezar presupune înlocuirea fiecărei litere din alfabet cu litera obținută prin deplasarea ciclică cu trei poziții a literelor alfabetului.

De exemplu:

text clar : meet me after the party

text cifrat : PHHW PH DIWHU WKH SDUWB

Avem așadar corespondența:

text clar: a b c d e f g h i j k l m n o p q r s t u v w x y z

text cifrat: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Dacă echivalentele numerice ale literelor sunt a = 1, b = 2, …, z = 26, rezultă $C = F(p) = (p + 3) \bmod 26$

unde p reprezintă litera alfabetului (text clar), iar F este litera cifrată a lui p.

[6] http://webhost.uoradea.ro/cpopescu/cryptography/Cursul4.pdf

1. INTRODUCERE

SISTEME CYBER-FIZICE (CPS)

Când discutăm despre securitatea în general, ne putem referi la multe lucruri, fiind o chestiune de perspectivă.

- fiabilitatea sistemului
- toleranța la eroare
- rezistență

VS

- asigurarea elementelor hardware
- siguranța datelor

CPS - concepute ca o rețea de dispozitive interconectate cu intrare și ieșire fizică și reprezintă o nouă direcție în lumea sistemelor de informare.

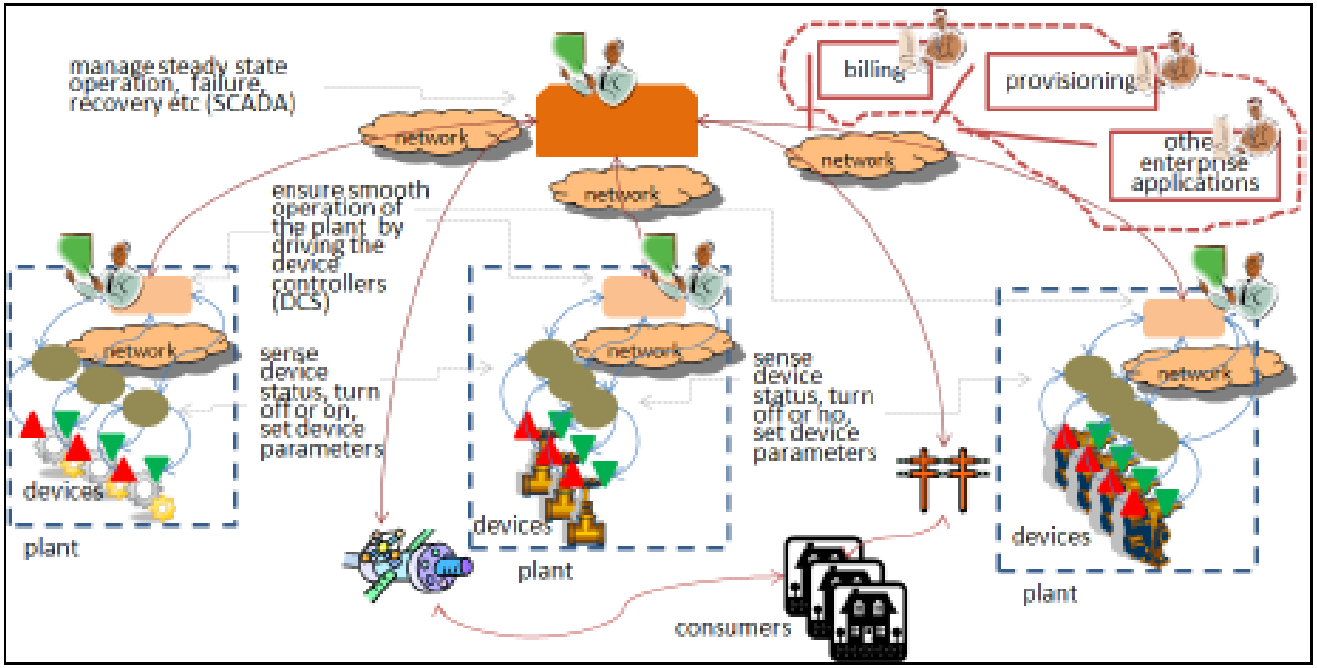
Termenul CPS sugerează interacțiunea dintre lumea reală și sistemele de informații.

[1] A. Burns, J. McDermid, J. Dobson, "On the Meaning of Safety and Security", The Computer Journal, Vol. 35, No. 1, 1992

1. INTRODUCERE

SISTEME CYBER-FIZICE (CPS)

CPS nu sunt doar aplicații desktop și nici nu sunt sistemele tradiționale în timp real, aduc un plus față de sistemele clasice –componentele lor informatice și fizice sunt integrate pentru învățare și adaptare, auto- organizare și performanță [2, 3]



CPS - rețea de dispozitive interconectate [preluare din 4]

[2] Partha Pal, Rick Schantz, Kurt Rohloff, Joseph Loyall, ”Cyber-Physical Systems Security – Challanges and Research”, BBN Technologies, Cambridge

[3] Dr. Clifford Neuman, ”Challanges in Security for Cyber-Physical Systems” http://cimic.rutgers.edu/positionPapers/CPS-Neuman.pdf

[4] Laura Vegh, Raport de cercetare nr.1, UTC-N

2. SECURITATEA ÎN CPS

Fiind compuse din elemente hardware și software ce le permite să se conecteze cu mediul, numeroasele facilități pe care le aduc, au făcut din CPS candidatul perfect când vine vorba de controlul proceselor critice.

Din acest motiv , orice compromis în securitatea CPS-ului ar avea consecințe serioase.

Securizarea CPS este cu atât mai dificilă cu cât CPS înglobează diferite tipuri de sisteme și procese. Din acest motiv modulul de securizare a informațiilor face parte integrantă din CPS.

Exemple de CPS

- rețelele de distribuție a energiei electrice ,
- rețele de distribuție a gazelor naturale,
- servicii medicale de urgență

2. SECURITATEA ÎN CPS

Principalele amenințări de securitate sunt de mare interes în domeniul CPS.

Confidențialitatea , sau prevenirea accesului la informație de către persoane neautorizate sau sisteme, este un aspect important la proiectarea CPS și poate fi obținută prin **criptarea datelor** .

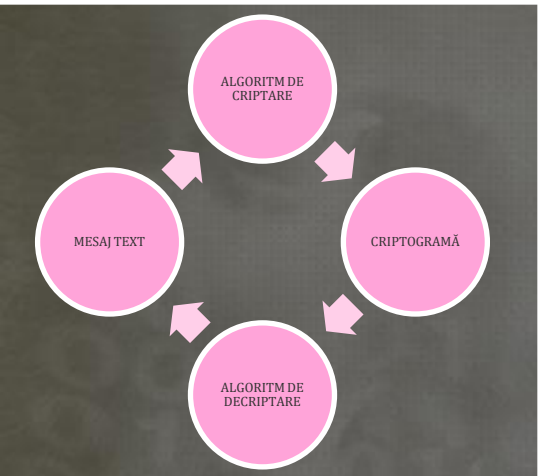
Integritatea se referă la asigurarea datelor în așa fel încât să nu poate fi modificată fără permisiune .

Disponibilitatea este , de asemenea, o cerință importantă în CPS, sistemul trebuie să fie disponibil ori de câte ori este nevoie - atât fizic cât și cibernetic.

Autenticitatea - tranzacțiile și comunicările sunt originale.

Din alt punct de vedere putem găsi un alt set de cerințe pentru securizarea CPS: **autentificare, securizarea stocării datelor, securizarea comunicării.**

3. CRIPTOGRAFIA



CRIPTOGRAFIA=ştiinţa scrierilor secrete (ştiinţa creării şi menţinerii mesajelor secrete, în sensul imposibiltăţii citirii lor de către neautorizaţi)

kryptos (ascuns)+ graphein (a scrie)

Mesaj (text) în clar (M) (plain/clear text) este mesajul ce urmează a fi secretizat; în criptografie M se numeşte scriere chiar dacă este un document de altă natură, de exemplu voce, imagine, date.

Mesaj cifrat (criptograma) (C) (cipher text) este mesajul secretizat, inaccesibil neavizaţilor.

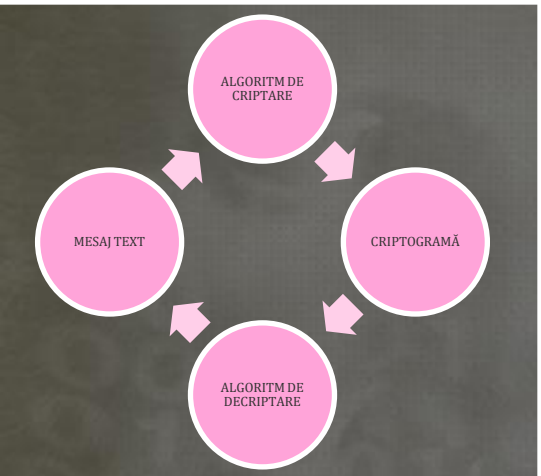
Criptare/cifrare (E) (encryption/enciphering) este procedeul de ”ascundere” a unui mesaj în clar în mesajul secretizat.

$$E(M)=C$$

Decriptare/descifrare (D) (decryption / deciphering) este procedeul de regăsire a mesajului în clar M din mesajul cifrat C.

$$D(C) = D(E(M))=M$$

3. CRIPTOGRAFIA



Criptograf (cryptographer) este persoana care se ocupă cu criptografia.

Algoritm criptografic / cifru (cryptographic algorithm / cipher) este funcţia sau funcţiile matematice utilizate pentru criptare / decriptare; în general exista două funcţii: una pentru criptare (E) şi alta pentru decriptare (D).

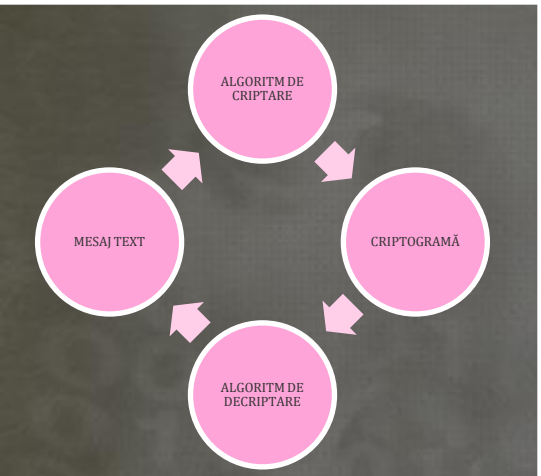
Cheia criptografica (K) *(key)* este mărimea (în majoritatea cazurilor secretă) necesară realizării criptării şi decriptării.

Criptosistem (cryptosistem) este sistemul format din:

- algoritm
- toate mesajele în clar (M)
- toate textele cifrate (C)
- toate cheile (K).

Criptanaliza (cryptanalysis) este ştiinţa spargerii cifrurilor, deci a obţinerii mesajelor în clar (M) sau a cheii (K) din mesajul cifrat(C)**.**

3. CRIPTOGRAFIA



Criptanalist (cryptanayst) este persoana care se ocupă cu criptanaliza.

Atac(attack) este încercarea / tentativa criptanalitică.

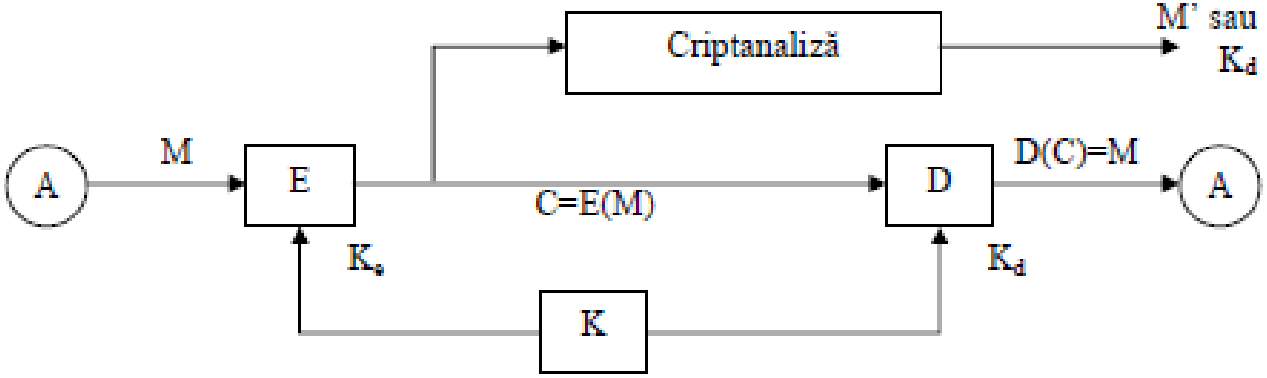
Criptologie(cryptology) este ştiinţa care se ocupă atât de criptografie cât şi de criptanaliză.

Criptolog (cryptologist) este persoana care se ocupă cu criptologia.

Steganografia(steganography) este tehnica ascunderii mesajelor secrete în alte mesaje, în aşa fel încât existenţa mesajelor secrete să fie invizibilă.

3. CRIPTOGRAFIA

CRIPTOSISTEMUL



Schema bloc a unui criptosistem [preluare din 5]

A,B - entităţi ce emit, recepţionează sau manipulează informaţia
E - funcţia de criptare(cifrare)
D - funcţia de decriptare(descifrare)
M - spaţiul mesajelor în clar
C - spaţiul criptogramelor(text cifrat)
K - spaţiul cheilor
Ke - spaţiul cheilor de criptare
Kd - spaţiul cheilor de decriptare

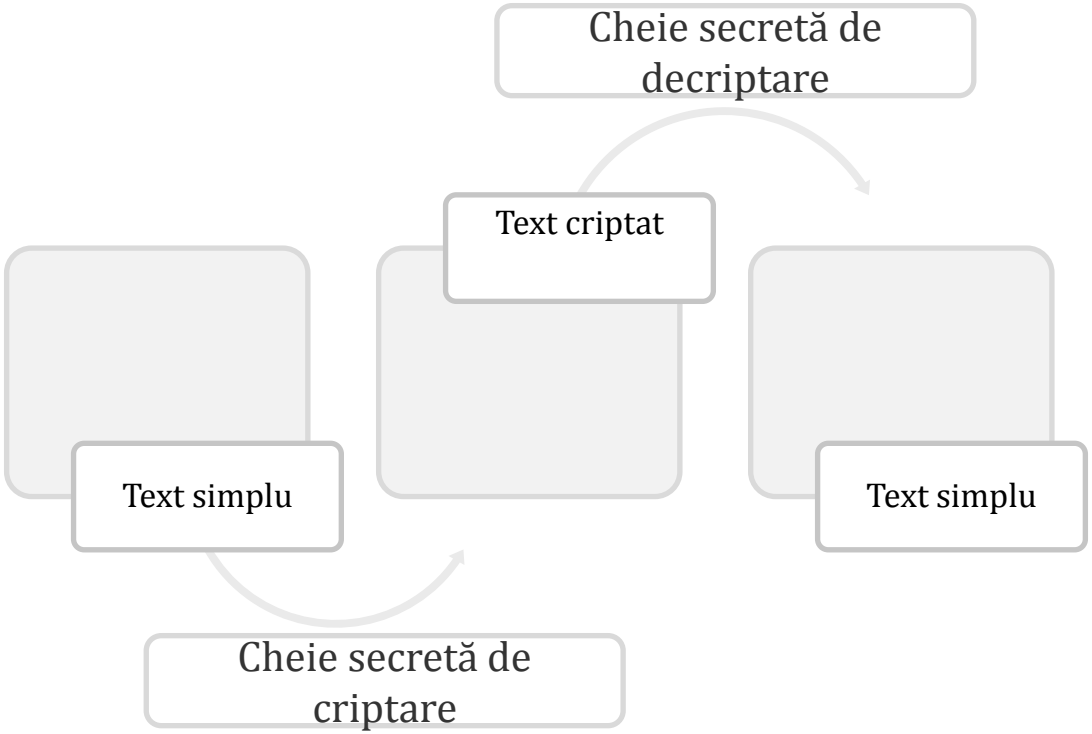
Rolul unui criptosistem este de a preveni sau detecta activităţile nepermise dintr-un sistem informatic.

[5] http://ro.scribd.com/doc/253171554/Criptare-Curs-An6#scribd

3. CRIPTOGRAFIA

CRIPTAREA CU CHEIE CRIPTOGRAFICĂ

Criptosistemele cu chei simetrice sunt criptosistemele pentru care cheile folosite la criptare şi decriptare sunt identice, de unde şi denumirea de criptosisteme cu chei simetrice.



Problema care se pune este existenţa unui canal sigur. Pentru n utilizatori rezultă n(n-1)/2 legături bidirecţionale.
Exemple: DES (Data Encryption Standard), **AES** (Advanced Encryption Standard), **TDES** (Triple-Data Encryption Standard).

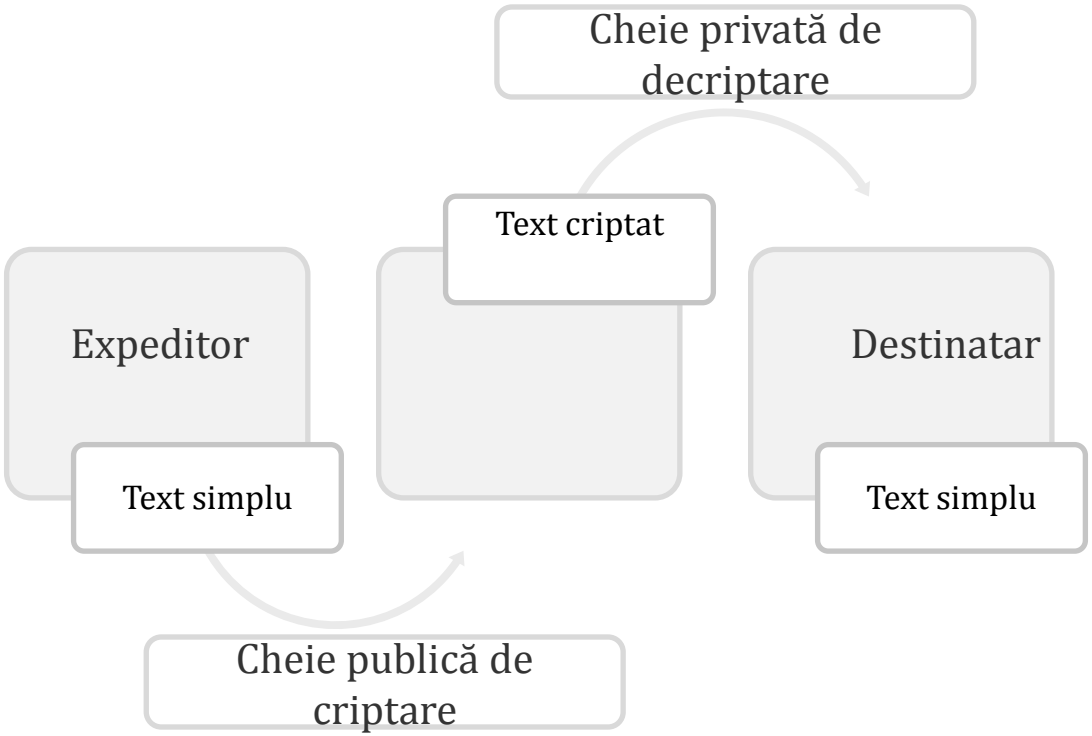
[5] http://ro.scribd.com/doc/253171554/Criptare-Curs-An6#scribd

3. CRIPTOGRAFIA

CRIPTAREA CU CHEIE PUBLICĂ (ASIMETRICĂ)

CRIPTOGRAFIA ASIMETRICĂ foloseşte două chei, diferite, una pentru cifrare, alta pentru descifrare. Deoarece este imposibilă deducerea unei chei din cealaltă, una din chei este făcută publicã fiind pusă la dispoziţia oricui doreşte să transmită un mesaj cifrat.

Doar destinatarul, care deţine cea de-a doua cheie, poate descifra şi utiliza mesajul.

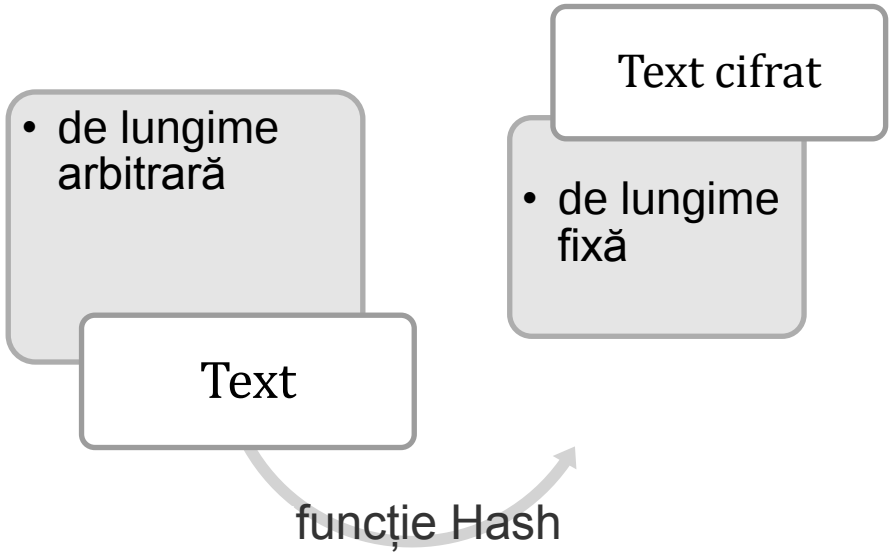


[5] http://ro.scribd.com/doc/253171554/Criptare-Curs-An6#scribd

3. CRIPTOGRAFIA

Funcții HASH

- funcții definite pe o mulțime cu multe elemente (posibil infinită) cu valori într-o mulțime cu un număr fix și mai redus de elemente.
- nu sunt inversabile
- folosite pentru a accelera căutările în tabele, cum este cazul în bazele de date mari sau comparările de date
- valoarea unei funcții hash este denumită rezumat, valoare hash, cod hash, sumă hash sau doar hash
- folosite drept componente în schemele de semnătură digitală.



Proprietăți: cost scăzut, determinism, uniformitate, domeniu de variație mare, normalizarea datelor

4. STEGANOGRAFIA

GENERALITĂȚI

DEFINIȚIE: arta de a comunica într-un mod ce ascunde existența comunicării.

Steganografie înseamnă în limba greacă "scris ascuns". Scopul steganografiei este de a ascunde mesajele în interiorul unor comunicări inofensive astfel încât acestea să nu fie detectate.

Steganografia nu este criptografie, mesajele nefiind codificate ci doar ascunse într-un mod în care detectarea lor este aproape imposibilă.

În anul 440 î.c., regele Darius din Susa a tatuat pe scalpul unui curier un mesaj secret destinat ginerelui său Aristogoras din Milet, mesaj ce îndemna la o revoltă împotriva perşilor. Mesajul a ajuns în Milet după ce curierului i-a crescut părul, acesta reuşind astfel să treacă nedetectat de perşi.

http://despretot.info/2012/10/steganografia-definitie-dex/

4. STEGANOGRAFIA

GENERALITĂȚI

Metodele **steganografice** pot fi grupate în:

steganografia prin injecţie – datele care se doresc a fi mascate sunt plasate în interiorul unui fişier text, fişier software, fişier audio sau video. Această metodă duce la creşterea dimensiunii iniţiale a fişierului cu cea corespunzătoare a informaţiilor injectate;

steganografia prin substituţie – informaţia este plasată prin înlocuirea unor părţi nesemnificative ale fişierelor gazdă, astfel încât la procesarea prin aplicaţiile software native (de exemplu fişierele mp3 procesate cu Winamp) să nu apară indicii despre faptul că acestea ar fi fost alterate;

steganografia prin propagare – se utilizează o aplicaţie software la intrarea căreia se furnizează informaţia utilă şi ce are ca rezultat un fişier din tipurile:text, imagine, video, audio. Fişierul este creat de aplicaţie pe baza informaţiei utile.

http://despretot.info/2012/10/steganografia-definitie-dex/

4. STEGANOGRAFIA

STEGANOGRAFIA TEHNICĂ

Securitatea sistemului steganografic depinde de locul ce va fi modificat în așa fel încât să ascundă datele și distorsiunile ce ar putea să apară în timpul procesului.

Designul sistemului steganografic trebuie să țină cont de aceste elemente: alegerea unei ascunzători potrivite și găsirea unei modalități de modificare imperceptibilă a mesajului original folosind algoritmi specifici.

Cea mai comună modalitate de transmitere a mesajelor este cu ajutorul imaginilor.

Faptul că se lucrează ușor cu imagini nu înseamnă că nivelul de securizare este scăzut.

În funcție de modul în care se face inserția și extracția mesajului tehnicile stego se împart în: sisteme de substituție, tehnici de distorsionare, metode statistice, etc.

http://despretot.info/2012/10/steganografia-definitie-dex/

4. STEGANOGRAFIA

STEGANOGRAFIA TEHNICĂ

Exemplu

Imagine nealterată

Imagine Stego

4. STEGANOGRAFIA

STEGANOGRAFIA TEHNICĂ

Exemplu: TEHNICI de substituție

LSB este cea mai comună tehnică de steganografie, fiind utilizată în general în fișiere în care unii biți sunt mult mai susceptibili la alterare decât alții.

Fișierele audio sau video reprezintă țintele preferate pentru această tehnică. Prin LSB sunt schimbați doar cei mai puțin semnificativi biți din mediul respectiv.

Folosită pentru a ascunde informație în imaginile grafice. Cele mai simple formate (bmp, pcx, gif) exprimă culorile ca biți, care apoi vor descrie pixelii dintr-o imagine.

Concluzie: orice tehnică poate fi folosită când se definește designul sistemului steganografic. Există diverși algoritmi care pot fi folosiți pentru același tip de aplicație, singura limitare este dată detipul sistemului care trebuie să fie securizat și de resursele disponibile.

http://despretot.info/2012/10/steganografia-definitie-dex/

4. STEGANOGRAFIA

STEGANOGRAFIA LINGVISTICĂ

Este o ramură importantă a tehnicilor de ascundere a datelor de la schimbarea **formatării unui text existent**, sau **schimbarea cuvintelor în text**, pentru a genera secvențe de caractere aleatoare sau chiar folosind **regulile gramaticale** pentru a genera un text lizibil .

XML sau HTML este o altă posibilitate pentru ascunderea informației, folosind tag-urile. Dacă anumite tag-uri sunt deschise într-o succesiune anume, se interpretează ca fiind bit 0 iar dacă se folosește o altă secvență va fi interpretată ca fiind bit 1.

Exemple mai moderne de steganografie includ utilizarea de cerneală invizibilă, micropuncte, și watermarkingul digital.

http://despretot.info/2012/10/steganografia-definitie-dex/

5. CRIPTOGRAFIE+ STEGANOGRAFIE

O nouă tehnică de securizare a datelor este folosirea celor 2 tehnici în combinație.

Daca **criptografia** este sigură în funcție de sistemul criptografic creat, securizând mesajul prin alterarea formei acestuia facând mesajul de necitit fără cheia potrivită, **steganografia** securizează chiar existența mesajului ascunzându-l într-un fișier, poză, fișier audio sau video.

Astfel există multe aplicații în care se poate observa utilizarea combinată a metodelor pentru securizarea datelor biometrice sau e-banking [7, 8].

Datorită complexității sistemelor cyber-fizice, acestea necesită un sistem de securitate robust. Din acest motiv în momentul în care se pune accentul pe securizrea datelor metoda combinată este cea mai potrivită în designul CPS.

[7] P. Thiyagarajan, G. Aghila, ”Qualitative Analysis of Dynamic Pattern based Steganography Algorithm in providing E-banking Security”, Disponibil la: http://www.idrbt.ac.in/PDFs/THIYAGARAJAN.pdf
[8] Sonsare Pravin, ”Stegano-Cryptosystem for Enhancing Biometric-feature Security with RSA”, International Conference on Information and Network Technology, Singapore, 2011

6. SEMNĂTURA DIGITALĂ

Poate fi folosită în scopul autentificării și integrității CPS.

Chiar și în sisteme criptate semnătura digitală își poate dovedi utilitatea. Este posibil să modificăm datele fără a le înțelege. În astfel de cazuri mesajul ajunge la decriptor alterat fără a avea posibilitatea de a verifica integritatea mesajului.

În acest scenariu, semnătura digitală este extrem de importantă, deoarece prin modificarea mesajului se alterează și semnătura.

CPS pot beneficia de semnături sub diverse forme, în cazul nostru o folosim pentru autentificarea și integritatea sistemului.

De cele mai multe ori mesajul este semnat de un singur utilizator. Există momente cand documentele au mai mulți semnatari (algoritmul ElGamal).

6. SEMNĂTURA DIGITALĂ

Faza1 - **generarea cheii** urmează **faza semnăturii** – a doua fază a algoritmului iar ultima fază este cea de **verificare** a acesteia.

Nivelul de securizare a datelor este dat de cheia generată deoarece aceasta nu se dezvăluie publicului larg.

Urmărirea inversă a cheii este practic imposibilă.

6. CONCLUZII

- S-au descris principalele metode pentru a asigura securitatea informațiilor.

- Accentul a fost pus pe aspectele principale ale fiecărei dintre metode, scopul fiind de a le înțelege mai bine cum funcţionează, care sunt principalele diferente între acestea şi locul lor în cadrul zonei de securitate a informațiilor.

- Sisteme de CPS sunt sisteme complexe, puternice, care oferă numeroase facilități .

- Ele sunt folosite în multe aplicații critice, care au nevoie de astfel de arhitecturi de securitate puternice.

BIBLIOGRAFIE selectivă

.

[1] A. Burns, J. McDermid, J. Dobson, “On the Meaning of Safety and Security”, The Computer Journal, Vol. 35, No. 1, 1992
[2] Partha Pal, Rick Schantz, Kurt Rohloff, Joseph Loyall, ”Cyber-Physical Systems Security – Challanges and Research”, BBN Technologies, Cambridge
[3] Dr. Clifford Neuman, ”Challanges in Security for Cyber-Physical Systems” http://cimic.rutgers.edu/positionPapers/CPS-Neuman.pdf
[4] Laura Vegh, Raport de cercetare nr.1, UTC-N
[5] http://ro.scribd.com/doc/253171554/Criptare-Curs-An6#scribd
[6] webhost.uoradea.ro/cpopescu/cryptography/Cursul4.pdf
[7] P. Thiyagarajan, G. Aghila, ”Qualitative Analysis of Dynamic Pattern based Steganography Algorithm in providing E-banking Security”, Disponibil la: http://www.idrbt.ac.in/PDFs/THIYAGARAJAN.pdf
[8] Sonsare Pravin, ”Stegano-Cryptosystem for Enhancing Biometric-feature Security with RSA”, International Conference on Information and Network Technology, Singapore, 2011
[9] http://despretot.info/2012/10/steganografia-definitie-dex/

.

YD PXOWXPHVF SHQWUX DWHQWLH !!

.

Vă multumesc pentru atenție!