Dezvoltarea unei aplicatii pentru criptarea datelor utilizand arhitectura JCA (Java Criptography Architecture)

Introducere – tema lucrarii, importanta ei in contextual actual, o enumerare a tehnologiilor utilizate pentru dezvoltarea aplicatiei

Capitolul 1 – Prezentarea generala a tehnologiilor utilizate – Java (JCA, swing)

Capitolul 2 – Arhitectura aplicatiei – baze de date, clase, modul utilizator, admin – clase utilizate. Secvente de cod.

Capitolul 3 – Functionalitatea aplicatiei (un fel de ghid de utilizare)/

Capitolul 4 - descrierea algoritmilor criptografici

Concluzii – tema lucrarii, directii viitoare de dezvoltare – criptare video/audio ca directie

Introducere – tema lucrarii, importanta ei in contextual actual, o enumerare a tehnologiilor utilizate pentru dezvoltarea aplicatiei

Introducere

Criptografia este arta si stiinta prepararii codate sau protejate a comunicatiilor care trebuie sa fie inteligibile doar pentru persoana care are o cheie in posesie. Criptografia (greaca, *kryptos*, "ascuns", *graphos* "a scrie" ) se refera la procesul de a comunica in sau de a descifra scrieri ascunse (coduri sau cifruri), dar si la folosirea de coduri pentru a converti date computerizate in asa fel incat numai un recipient anume sa le poata citi folosind o cheie (criptare). Criptografii definesc ca text clar sau text simplu o comunicatie originala. Odata ce comunicatia originala a fost criptata, rezultatul este cunoscut ca text cifrat sau criptograma. Procesul de cifrare implica de obicei un algoritm si o cheie. Un algoritm de criptare este o metoda particulara de amestecare – un program de calculator sau un set de instructiuni scrise. Cheia specifica procesul de amestecare. Comunicatia originala poate fi un mesaj scris sau difuzat sau un set de date digitale.

In sensul mai larg, criptografia include folosirea de mesaje ascunse, cifruri si coduri. Mesajele ascunse, asemeni celor ascunse in text la vedere sau celor scrise cu cerneala invizibila , depinde de succesul lor de a nu fi suspectate. Odata ce sunt descoperite, sunt in mod frecvent usor de descifrat. Codurile, in care cuvintele, numerele sau simbolurile reprezinta cuvinte si fraze, sunt de obicei imposibil de citit fara cheia dictionarului. Criptografia include, de asemenea, folosirea criptarii computerizate pentru protejarea transmisiilor de date si mesaje.

Criptografia – proces general:

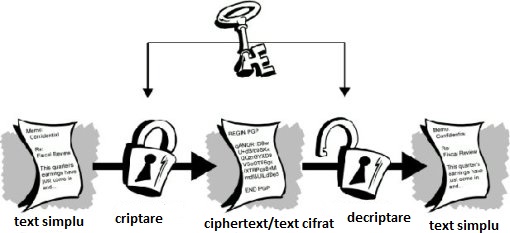


Fig.1-Criptografia – descriere proces

* 1. Istoric

Inainte de epoca moderna, criptografia se ocupa doar cu asigurarea confidentialitatii mesajelor si inversul acestui proces pentru a face mesajul imposibil de inteles pentru cei care intercepteaza mesajul si nu detin cheia necesara decriptarii mesajului. Cele mai vechi forme de scriere secretizata necesitau doar putin mai mult decat unelte de scris si hartie deoarece majoritatea oamenilor nu stiau sa citeasca. Cu timpul, complexitatea criptografiei a crescut deoarece a crescut si alfabetizarea. Principalele tipuri clasice de cifruri sunt [cifrurile cu transpoziție](https://ro.wikipedia.org/w/index.php?title=Cifru_cu_transpozi%C8%9Bie&action=edit&redlink=1), care modifică ordinea literelor dintr-un mesaj (de exemplu „ajutor” devine „ojartu” într-o schemă trivială de rearanjare), și [cifrurile cu substituție](https://ro.wikipedia.org/w/index.php?title=Cifru_cu_substitu%C8%9Bie&action=edit&redlink=1), care înlocuiesc sistematic litere sau grupuri de litere cu alte litere și grupuri de litere (de exemplu, „conexiune” devine „dpofyjvof” înlocuind fiecare literă cu următoarea din alfabet). Versiuni simple ale celor două tipuri de cifruri ofereau un grad mic de confidențialitate în cazul oponenților instruiți. Unul din primele cifruri cu substituție a fost [Cifrul lui Cezar](https://ro.wikipedia.org/wiki/Cifrul_lui_Cezar), în care fiecare literă din textul clar era înlocuită cu o literă aflată la un număr fix de poziții distanță de ea în alfabet. Cifrul a fost denumit astfel după [Iulius Cezar](https://ro.wikipedia.org/wiki/Iulius_Cezar) despre care se spune că l-a folosit, cu o deplasare de 3, în comunicația cu generalii săi în timpul campaniilor militare. In ultimele 2 decenii, domeniul s-a extins dincolo de problemele de confidentialitate si include, printre altele, si tehnici de verificare a integritatii mesajului, autentificarea trimitatorului si a receptorului, semnatura electronica, calcule securizate.

* 1. Importanta criptografiei in contextual actual

Astazi, majoritatea comunicatiilor lasa un fel de urma inregistrata. De exemplu, comunicatiile telefonice, inclusive faxurile si mesajele e-mail, produc o inregistrare a numarului de telefon apelat si timpul la care a fost apelat. Tranzactiile financiare, istoricul medical, alegerea filmelor inchiriate si chiar si alegerea mancarii pot fi urmarite cu chitantele cardului bancar sau inregistrarile asigurarii. De fiecare data cand cineva foloseste un telefon sau un card bancar, compania de telefoane sau institutia financiara tine o inregistrare a numarului apelat sau a sumei tranzactionate, a locatiei si a datei. In viitor, pe masura ce retelele telefonice devin digitale, chiar si conversatiile insesi pot fi inregistrate si stocate. Toate acestea duc catre o mai mare confidentialitate. Abilitatea de a cripta date, comunicatii si alte informatii le da indivizilor puterea de a isi restaura confidentialitatea personala.

Criptografia ofera mai mult decat confidentialitate, totusi. Criptografia protejeaza si sistemele bancare mondiale. Multe banci si alte institutii financiare isi conduc afacerile pe canale deschise, precum internetul. Fara abilitatea de a proteja tranzactiile si comunicatiile bancare, criminalii pot interveni in tranzactii si pot fura bani fara a lasa o urma.

* 1. Tehnologii utilizate

Toate aspectele mentionate mai sus duc la concluzia ca criptografia este o componenta din ce in ce mai necesara desfasurarii activitatilor zilnice individuale, dar si a activitatilor la nivel de system.

Influentata de tendinta de digitalizare si de evolutia tehnologica rapida, imi propun prin aceasta lucrare implementarea unei astfel de aplicatii folosind API-ul oferit de limbajul de programare JAVA prin intermediul librariei JCA (Java Cryptography Architecture ). Aplicatia, inspirata dintr-o nevoie de a ascunde comunicatiile intre trimitator si receptor, se incadreaza in categoria produselor software destinate securizarii unui computer sau a unei retele.

In capitolul 1 sunt prezentate pe scurt tehnicile de criptografiere si sunt identificate si analizate solutiile oferite de aceasta la provocarile oferite de protejarea si securizarea datelor.

Capitolul 2 face o scurta introducere in lumea dezvoltarii de aplicatii software de securitate si prezinta tehnologiile folosite pentru atingerea obiectivului acestei lucrari. Acesta include limbajul de programare Java, libraria Java Criptography Architecture si setul de componente GUI JFC.

Capitolul 3 descrie in detaliu toate functionalitatile aplicatiei si metodele folosite pentru implementarea acestora.

Capitolul 4 pune accentual pe implementarea algoritmilor criptografici. Sunt prezentati principalii algoritmi de criptare pe tipuri de cheie utilizate si modul in care acestia au fost aplicati in procesul de implementare pentru a se potrivi contextului aplicatiei dezvoltate.

<http://dspace.cusat.ac.in/jspui/bitstream/123456789/2628/1/Cryptography%20and%20Security.pdf>

<https://ro.wikipedia.org/wiki/Criptografie>

https://profs.info.uaic.ro/~adiftene/Licenta/Licenta2013\_Nita%20Iulian-Alexandru.pdf

<https://en.wikipedia.org/wiki/Java_Cryptography_Architecture>

<https://www.webopedia.com/TERM/S/security_software.html>

<https://pdfs.semanticscholar.org/187d/26258dc57d794ce4badb094e64cf8d3f7d88.pdf>

<https://en.wikipedia.org/wiki/Symmetric-key_algorithm>

https://en.wikipedia.org/wiki/Advanced\_Encryption\_Standard

<https://www.lri.fr/~fmartignon/documenti/systemesecurite/5-AES.pdf>

<http://www.iusmentis.com/technology/encryption/des/>

<http://cs.indstate.edu/~schinta/blowfish.pdf>

<https://en.wikipedia.org/wiki/Public-key_cryptography>

<https://www.cs.utexas.edu/~byoung/cs361/lecture52.pdf>

<https://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1003_DSA.pdf>

<https://en.wikipedia.org/wiki/Digital_Signature_Algorithm>

https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

**Capitolul 4**

**Algoritmii criptografici**

Algoritmii de criptare sunt clasificati in doua grupe: algoritmi de criptare pe *cheie simetrica* (denumita si cheie secreta) si algoritmi de criptare pe *cheie asimetrica* (denumita si cheie publica).

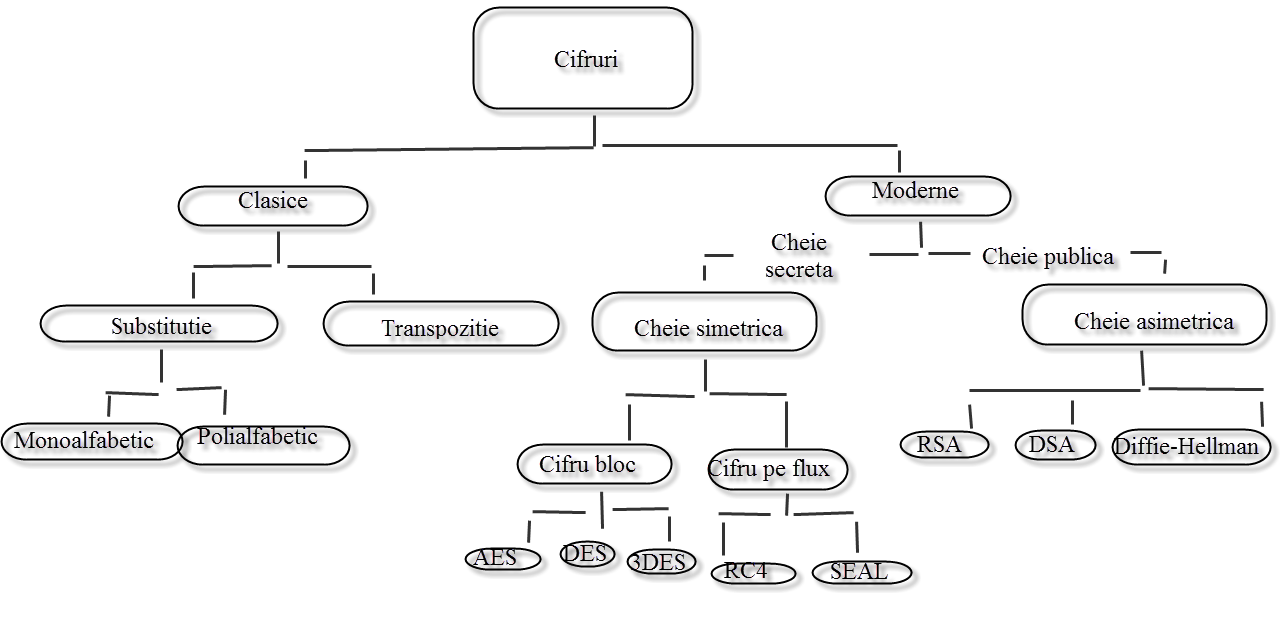
Criptarea pe cheie simetrica este o forma de criptosistem in care criptarea si decriptarea sunt executate folosind aceeasi cheie. Este cunoscuta si sub numele de criptare conventionala.

Criptarea asimetrica este o forma de criptosistem in care criptarea si decriptarea sunt executate folosind chei diferite – una cu o cheie publica si una cu o cheie privata. Este cunoscuta si sub numele de criptare pe cheie publica.

O cheie este un text numeric sau alfa numeric sau poate fi un symbol special. Cheia este folosita in momentul executarii criptarii pe textul in clar si in momentul executarii decriptarii textului cifrat. Selectia cheii in criptografie este foarte importanta avand in vedere faptul ca securitatea algoritmilor de criptare se bazeaza pe abilitatea cheii de a fi secreta, pe lungimea ei, a vectorului de initializare si cum functioneaza aceste toate componente la un loc.

Tehnicile de criptare asimetrica sunt de aproximativ 1000 de ori mai lente decat criptarea simetrica ceea ce le face impractice atunci cand se incearca criptarea portiunilor mari de date. De asemenea, pentru a ajunge la aceeasi putere de securitate ca cea simetrica, criptarea asimetrica trebuie sa foloseasca o cheie mai puternica decat tehnica de criptare simetrica. Clasificarea marilor tehnici de criptare este afisata in figura 1.12.

Figura 1.12 Clasificarea metodelor de criptare



4.1 Algoritmi pe cheie simetrica

Algoritmii pe cheie privata sunt algoritmi care folosesc aceeasi cheie criptografica si pentru criptare si pentru decriptare. Cheile pot fi identice sau poate fi o simpla transformare de facut intre 2 chei. Cheile, in practica, reprezinta un secret impartasit intre doua sau mai multe parti care pot fi folosite pentru a mentine privat un link informational.

Multe cifruri bloc modern sunt bazate pe o constructie propusa de Horst Feistel. Constructia lui Feistel face posibila construirea de functii inversabile din alte functii care nu sunt inversabile.

4.1.1 Rijndael Algorithm - AES (Advanced Encryption Standard)

AES, cunoscut si ca Rijndael este o specificatie pentru criptarea de date electronice stabilita de catre Institul National de Standarde si Tehnologii din US in 2001. AES este un subset al cifrului Rijndael dezvoltat de 2 criptografi belgieni, Vincent Rijmen si Joan Daemen, care au submis o propunere la NIST in timpul procesului de selectie AES. Rijndael este o familie de cifruri cu diferite chei si marimi de blocuri. Pentru AES, NIST a selectat 3 membri ai familiei Rijndael, fiecare cu o marime a blocului de 128 de biti, dar cu 3 lungimi diferite de cheie: 128, 192 si 256 de biti.

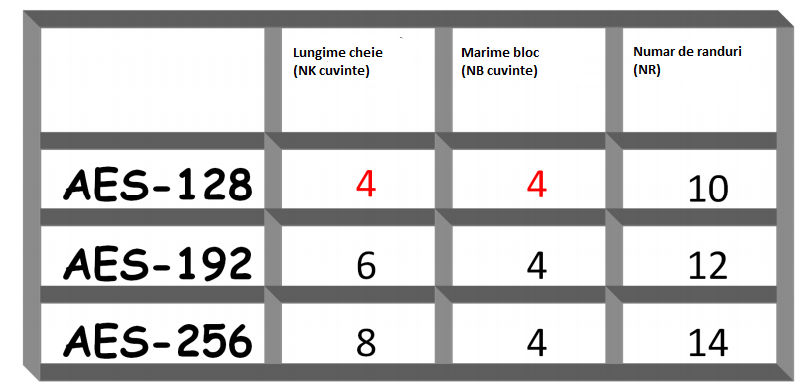
AES nu este un cifru Feistel. Acesta lucreaza in parallel peste tot blocul de intrare. Este construit pentru a fi efficient si in hardware, dar si in software pe o varietate de platforme. Este un cifru bloc care lucreaza iterative.

* Marime bloc: 128 de biti (dar si 192 sau 256 de biti)
* Lungime cheie: 128, 192 sau 256 de biti
* Numar de runde: 10, 12 sau 14
* Programarea cheii: 44, 52 sau 60 de subchei avand lungimea = 32 de biti

Fiecare runda (exceptand ultima) este o compozitie uniforma si paralela de 4 pasi:

* SubBytes (substitutie bit-cu-bit folosind un S-box)
* ShiftRows (o permutatie, care deplaseaza cyclic ultimele 3 randuri in stare)
* MixColumns (substitutie care foloseste campurile Galois, corps de Galois, GF (2 8)) arithmetic)
* AddRound key (bit-cu-bit XOR cu o cheie extinsa)

Figura 1.13 Parametri AES



Chei AES

Cu 128 de biti: 2 128 = 3.4 \* 10 38 chei posibile (un calculator care incearca 2 55 chei pe secunda are nevoie de 149.000 miliarde de ani ca sa sparga AES)

Cu 192 de biti: 2 192 = 6.2 \* 10 57 chei posibile

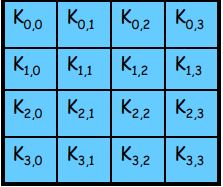
Cu 256 de biti: 2 256 = 1.1 \* 10 77 chei posibile

Cheie si bloc

Cheie cu lungime variabila (128, 192, 256 de biti) care este reprezentata cu o matrice (vector) de bytes cu 4 randuri si Nk coloane, Nk=lungime cheie/32.

1. Cheie de 128 de biti=16 bytes -> Nk=4
2. Cheie de 192 de biti=24 de biti -> Nk=6
3. Cheie de 256 de biti=32 de bytes -> Nk=8

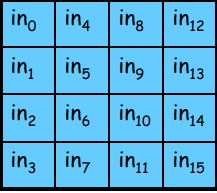
Figura 1.14 Matricea cheie



Bloc cu lungime de 128 de biti = 16 bytes. Este reprezentat de o matrice (vector) cu 4 randuri si Nb coloane, Nb = lungime bloc/32

* Bloc de 128 de biti=16 bytes -> Nb=4

Figura 1.15 Matricea bloc

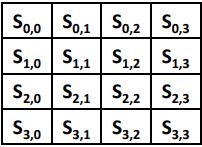


Stare

Intern, operatiile algoritmului AES sunt executate pe un array de bytes bidimensional numit *Stare*.

* Patru randuri, fiecare continand Nb bytes
* Nb coloane, constituite de cuvinte pe 32 de biti
* S r,c denota byte-ul in randul r si coloana c

Figura 1.16 Array-ul Stare



Design-ul lui Rijndael

* Operatii executate pe Stare (4 randuri de bytes)
* Cheia de 128 de biti este extinsa ca un array de 44 de intrari de cuvinte de 32 de biti; 4 cuvinte distincte servesc ca o cheie runda pentru fiecare runda; programarea cheii se bazeaza pe S-box.
* Algoritmi compusi din 2 straturi:

1. Difuzie liniara
2. Difuzie non-liniara
3. Amestec de cheie

4.1.2 Algoritmul DES (Data Encryption Standard)

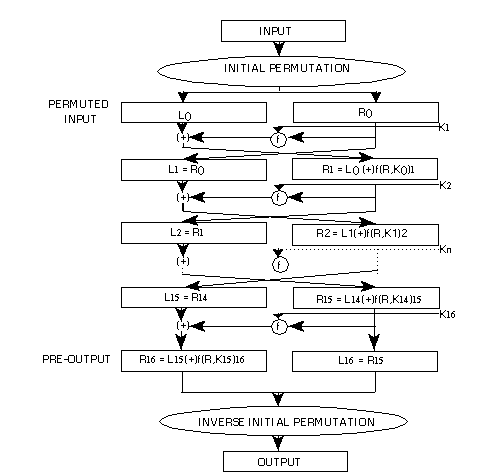
DES este o schema de criptare pe cheie private adoptata ca standard in USA in anul 1977. Foloseste o cheie de 56 de biti care astazi este considerate de multi ca insuficienta deoarece poate fi sparta folosind forta bruta cu un effort moderat. O variant numita Triplu-DES (TDES sau 3DES) foloseste o cheie mai lunga si este mai sigura, dar nu a devenit niciodata populara. AES este algoritmul care se asteapta sa superclaseze DES (si 3DES) ca algoritm standard de criptare.

DES a fost dezvoltat de comun accord in 1974 de catre IBM si guvernul USA (brevetul USA 3,962,539) pentru a seta un standard care se poate folosi pentru a securiza comunicatiile. Opereaza pe blocuri de 64 de biti folosind o cheie secreta care are o lungime de 56 de biti. Propunerea originala a folosit o cheie secreta cu o lungime de 64 de biti. Este crezut la scara larga ca indepartarea acestor 8 biti din cheie a fost facuta pentru a face posibila spargerea mesajelor de catre agentiile guvernamentale din US.

Criptarea unui bloc al mesajului se intampla in 16 runde sau stadii. De la cheia de intrare, 16 chei de 48 de biti sunt generate, cate una pentru fiecare runda. In fiecare runda, 8 asa-numite S-boxes sunt folosite. Aceste S-boxex sunt fixate in specificatia standardului. Folosind S-boxes, grupuri de cate sase biti sunt mapate pe grupuri de patru biti. Continutul acesto S-boxes a fost determinat de catre NSA (SUA). S-boxes par a fi umplute aleatoriu, dar nu este asa. Recent a fost descoperit ca aceste S-boxes, determinate in anii '70, sunt rezistente impotriva unui atac numit criptanaliza diferentiala care a fost observata in anii '90 pentru prima oara.

Blocul mesajului este impartit in doua jumatati. Jumatatea dreapta este marita de la 32 la 48 de biti folosind alt tabel fix. Rezultatul este combinat cu subcheia acelei runde folosind operatia XOR. Folosind S-boxes,, cei 48 de biti rezultati sunt transformati din nou in 32 de biti, care sunt din nou permutati ulterior folosind inca un tabel fix. Jumatatea dreapta rezultata este acum combinata cu jumatatea stanga folosind operatia XOR. In runda urmatoarea, aceasta combinatie este folosita ca noua jumatate stanga.

Figura 1.17 Permutari algoritm DES



4.1.3Algoritmul TDES/3DES (TripleDES)

Varianta de algoritm Triple-DES a fost dezvoltata dupa ce a devenit clar ca DES singur era prea usor de spart. Acesta foloseste trei chei DES de 56 de biti, dand in total o lungime a cheii de 168 de biti. Criptarea folosind 3DES este simpla:

1. Criptare folosind DES cu prima cheie de 56 de biti
2. Decriptare folosind DES cu a doua cheie de 56 de biti
3. Criptare folosind DES cu a treia cheie de 56 de biti

Deoarece Triple-DES aplica algoritmul DES de 3 ori (derivand numele de aici), Triple-DES are o durata de 3 ori mai mare ca DES. Decriptarea folosind Triple-DES este aceeasi ca si criptarea, doar ca este executata invers.

4.1.4 Algoritmul Blowfish

Cifrul algoritm simetric Blowfish cripteaza date bloc de 64 de biti odata. Algoritmul urmareste reteaua fiestal si este divizat in 3 parti mari:

Expansiunea cheii

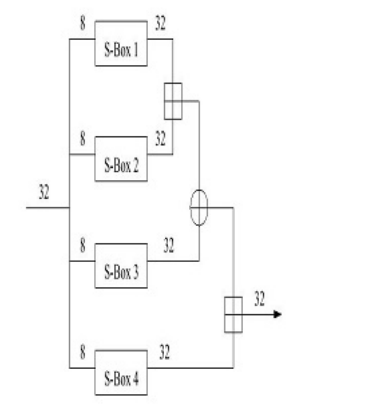
Criptarea de date

Decriptarea de date

4.1.4.1 Expansiunea cheii

Inaintea oricarei criptari si decriptari de date, aceste chei trebuie sa fie calculate inainte. Vectorul p este compus din subchei de 18 si 32 de biti: P1, P2,…,P18. Pentru 32 de biti, S-boxes sunt compuse din 256 de intrari fiecare.

Figura 1.18 Calcule expansiune cheie

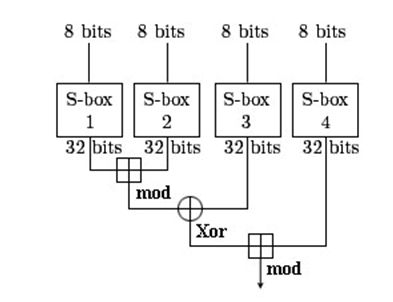


Subcheile sunt calculate si generate folosind algoritmul Blowfish:

1. Initializeaza intai array-ul P si pe urma cele 4 S-boxes, in ordine, cu un String fix. Acest String este compusa din cifrele hexazecimale ale lui pi (minus 3-ul initial): P1=0x243f6a88, P2=0x85a308d3, P3=0x13198a2e, P4=0x03707344, etc.
2. XOR P1 cu primii 32 de biti ai cheii, XOR P2 cu urmatorii 32 de biti ai cheii, samd, pentru toti bitii cheii (posibil pana la P14). Se repeat cyclic prin cheie pana cand pe intreg vectorul P a fost aplicat XOR cu bitii cheii.
3. Cripteaza Stringul de zero complet cu Blowfish, folosind cheile descrise mai sus.
4. Inlocuieste P1 si P2 cu outputul de la pasul anterior.
5. Cripteaza outputul de la pasul 3 folosinf algoritmul Blowfish cu subcheile modificate.
6. Inlocuieste P3 si P4 cu rezultatul de la pasul anterior.
7. Continua procesul, inlocuind toate intrarile vectorului P si apoi toate cele patru S-boxes in ordine, cu rezultatul continuu in schimbare a algoritmului Blowfish.

In total, 521 de iteratii sunt necesare pentru a genera toate sub-cheile necesare. Aplicatiile pot stoca sub-cheile, mai degraba decat sa execute acest process derivativ de multiple ori.

Figura 1.19 Blowfish



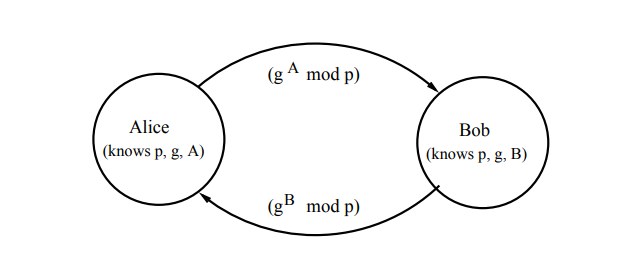
4.2 Algoritmi pe cheie asimetrica

Algoritmii pe cheie publica sunt ingrediente fundamentale de securitate in criptosisteme, aplicatii si protocoale. Acestia stau la baza diverselor standarde Internet, ca TLS, S/MIME, PGP si GPG. Unii algoritmi pe cheie publica ofera distributie de cheie si secretizare (ex: Diffie-Hellman schimb de cheie), altii ofera semnatura digitala (ex: Digital Signature Algorithm) si altii le ofera pe amandoua (ex: RSA).

4.2.1 Algoritmul Diffie-Hellman

Diffie-Hellman (1976) a fost prima metoda practica pentru stabilirea unui secret impartasit peste un canal de comunicare nesigur. Ideea este sa se agreeze asupra unei chei pentru ca 2 parti sa o poata folosi pentru criptare simetrica in asa fel incat cheia sa nu poata fi obtinuta de o alta parte neimplicata in schimbul informatiei.

Figura 1.20 Algoritmul Diffie-Hellman



Algoritmul este compus din urmatorii pasi:

1. Alice si Bob agreeaza asupra unui numar prim g si o baza g
2. Alice allege un numar secret a si ii trimite lui Bob (g a mod p)
3. Bob allege un numar secret b si ii trimite lui Alice (g b mod p)
4. Alice calculeaza ((gb mod p)a mod p)
5. Bob calculeaza ((ga mod p)b mod p)

Amandoi pot folosi acest numar si cheie. Se poate observa ca nu este nevoie ca p si g sa fie protejate.

4.2.2 Algoritmul DSA (Digital Signature Algorithm)

DSA a fost sugerat si standardizat de catre Institutul National de Standarde si Tehnologie (NIST), USA,. Este o variant eficienta a schemei de semnare ElGamal. Schema de semnare ElGamal are cateva dezavantaje pe care DSA le poate repara. Semnatura DSA are lungimea in biti de 320, iar verificarea acesteia necesita doar 2 operatii matematice modulare cu exponenti de lungime 160 de biti.

Generarea cheii are 2 faze. Prima faza este o alegere a parametrilor algoritm care poate fi impartasita intre utilizatori diferiti ai sistemului, in timp ce a doua faza calculeaza cheia publica si cheia privata pentru un singur utilizator.

* Generarea parametrului:

1. Se allege o functie criptografica hash H aprobata.
2. Se decide o lungime de cheie L si N. Aceasta este prima masura a puterii criptografice a cheii
3. Se allege u N-bit prim q
4. Se allege un L-bit prim p astfel incat p-1 este un multiplu de q
5. Se allege g, numar a carui ordine multiplicative modulo p este q.
6. Parametrii algoritm (p, q, g) pot fi impartasiti intre diferiti useri ai sistemului

* Chei per-utilizator:

Fiind dat un set de parametric, a 2 a faza calculeaza cheia publica si cheia private pentru un singur utilizator:

1. Se allege o cheie secreta x dupa o metoda aleatory, unde 0<x<q
2. Se calculeaza cheia publica y=g x mod p

Semnarea

Fie H o functie de hash si m mesajul:

* 1. Se genereaza o valoare per-mesaj aleatory k unde 1< k < q
  2. Se calculeaza r = (gk mod p) mod q
  3. In cazul putin probabil in care r=0, se incepe din nou cu un aleatoriu k diferit
  4. Se calculeaza s = k -1 (H(m) +xr) mod q
  5. In cazul putin probabil in care s=0, se incepe din nou cu un aleatoriu k diferit

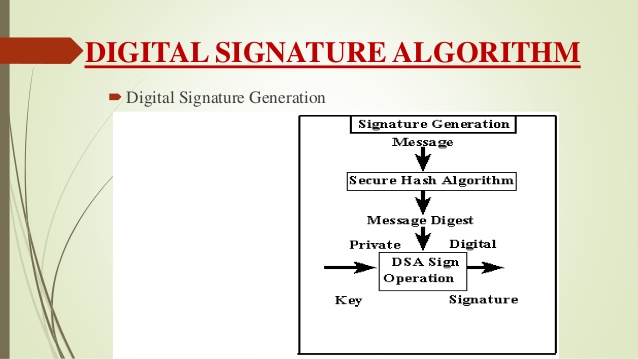
Semnatura este (r, s).

* Verificarea

1. Se respinge semantura daca 0 < r < q sau 0 < s < q nu este satisfacuta
2. Se calculeaza w = s -1 mod q
3. Se calculeaza u1 = H(m) \* w mod q
4. Se calculeaza u2 = r \* w mod q
5. Se calculeaza v = (g u1 y u2 mod p) mod q

Semnatura este valida daca si numai daca v = r.

Figura 1.21 DSA

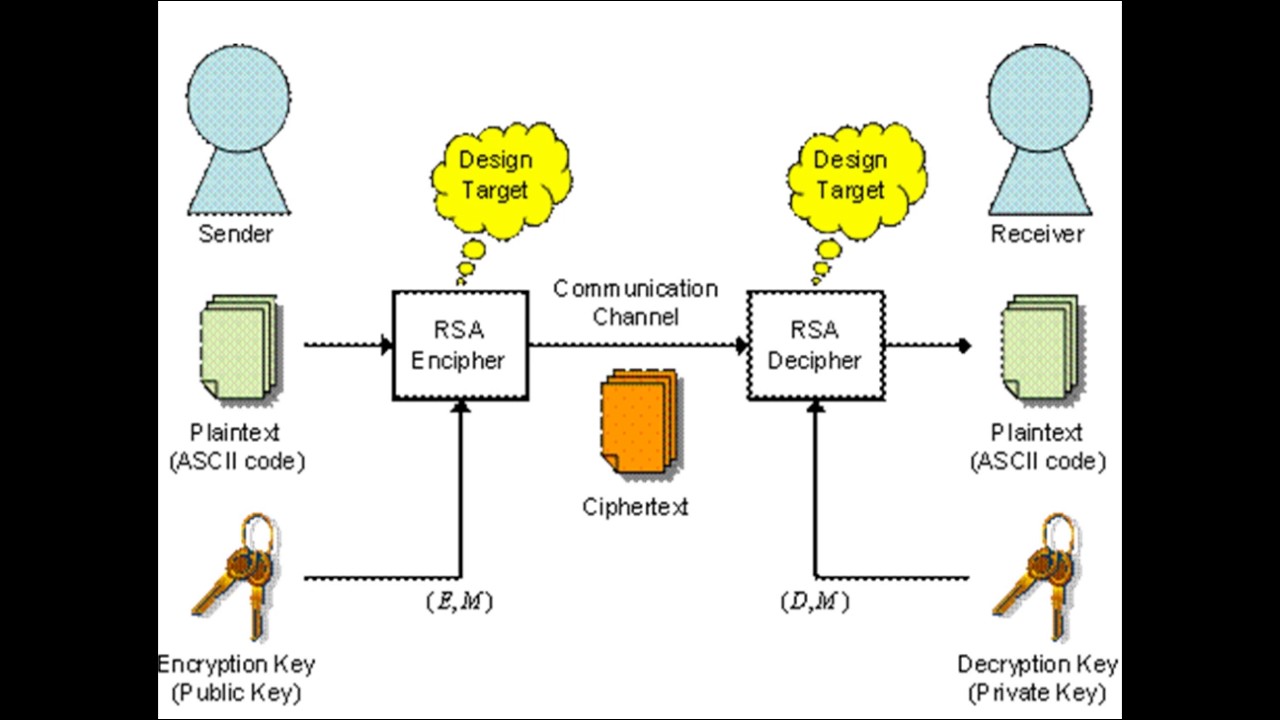


4.2.3 Algoritmul RSA (Rivest-Shamir-Adleman)

RSA a fost prima data descris in 1977 de catre Ron Rivest, Adi Shamir si Leonard Adleman, membri ai Institutului de Tehnologie Massachusetts.

Ideea algoritmului RSA se bazeaza pe faptul ca e dificil sa factorizezi un nr intreg mare. Cheia publica este formata din 2 numere unde unul dintre ele este multiplicarea a doua numere prime mari. Iar cheia private este de asemenea derivate din cele 2 numere prime. Deci, daca cineva poate factorize numarul mare, cheia private este compromisa. Aasadar, puterea de criptare sta complet in marimea cheii is daca se dubleaza sau tripleaza marimea cheii, puterea de criptare creste exponential. Cheile RSA sunt tipic cuprinse intre 1024 si 2048 de biti lungime, dar expertii cred ca cheile de 1024 de biti pot fi sparte in viitorul apropiat.

Figura 1.21 Algoritmul RSA



4.3 Concluzii

In contextul criptografiei, algoritmii criptografici reprezinta unealta asigurarii confidentialitatii datelor. Este destul de clar ca folosind algoritmi criptografici pentru schimb de cheie ca Diffie-Hellman pana la aplicarea de semnaturi digitale pentru a autentifica utilizatorul si continutul informatiei sunt elemente de conexiune importanta pentru sporirea securitatii sistemului, a informatiei, precum si a retelei.