**AES գաղտնագրում**

Գաղտնագրման համար AES ալգորիթմում կիրառվում են տվյալների ձևափոխության հետևյալ գործընթացները՝

1. ExpandKey - Բոլոր փուլերի համար փուլային բանալիների հաշվում:

2. SubBytes - Փոխարինման աղյուսակի միջոցով բայթերի փոխարինում:

3. ShiftRows - Վիճակում տողերի, տարբեր քանակությամբ, ցիկլիկ տեղաշարժ:

4. MixColumns - Վիճակի յուրաքանչյուր սյունյակում տվյալների խառնում:

5. AddRoundKey - Փուլի բանալու գումարումը վիճակին:

Գաղտնագրումը տեղի է ունենում նկ. 1-ում պատկերված ալգորիթմով:

**SubBytes ձևափոխությունը**

SubBytes ձևափոխությունը կայանում է վիճակի ամեն {xy} բայթը (որտեղ x և y 16-ական համակարգի թվեր են), աղ. 1-ի համաձայն, մեկ քայլով փոխարինման մեջ:

**ShiftRows** **ձևափոխությունը**

ShiftRows ձևափոխությունը իրենից ներկայացնում է վիճակի տողերի ցիկլիկտեղաշարժ դեպի ձախ: Առաջին տողը մնում է նափոփոխ, երկրորդում կատարվում է տեղաշարժ մեկ բայթով, երրորդում 2 բայթով, չորրորդում՝ 3:

**MixColumns ձևափոխությունը**

MixColumns ձևափոխության ժամանակ կատարվում է 4-րդ աստիճանի քառակուսային մատրիցի բազմապատկում վիճակի յուրաքանչյուր սյունյակի հետ: Յուրաքանչյուր սյունյակի հետ գործողությունը կատարվում է առանձին:

**AddRoundKey** **ձևափոխությունը**

AddRoundKey ձևափոխության ժամանակ փուլային բանալու 32-բիթանոց բառերը XOR բիթային գործողության միջոցով գումարվում են վիճակի սյուներին: Յուրաքանչյուր սյունյակի հետ գործողությունը կատարվում է առանձին:

**ExpandKey** **գործընթացը**

AES ալգորիթմում փուլային բանալիները գեներացվում են գաղտնագրման բանալու հիման վրա՝ ExpandKey գործընթացի միջոցով: ExpandKey գործընթացը ստեղծում է Nb \* (Nr + 1) բառ, որտեղ Nb-ն բլոկում բառերի քանակն է, Nr-ը՝ փուլերի քանակը: Ալգորիթմին անհրաժեշտ է Nb երկարությամբ սկզբնական բանալի, ինչպես նաև Nr փուլերից յուրաքանչյուրը պահանջում է Nb բառերից կազմված բանալի:

**AES վերծանում**

Վերծանման ժամանակ բոլոր ձևափոխությունները կատարվում են հակառակ հերթականությամբ: Գոյություն ունեցող գաղտնագրող ձևոփոխությունների փոխարեն օգտագործվում են հետևյալ հակադարձ ձևափոխությունները՝

1. InvSubBytes - Բայթերի փոխարինում հակադարձ փոխարինման աղյուսակի միջոցով,

2. InvShiftRows - Վիճակում տողերի ցիկլիկ տեղաշարժ տարբեր քայլերով,

3. InvMixColumns - Վիճակի յուրաքանչյուր սյունյակում տվյալների խառնում:

ExpandKey և AddRoundKey գործընթացները մնում են անփոփոխ: Փուլի բանալիները օգտագործվում են հակառակ հերթականությամբ: Վերծանման ալգորիթմը ներկայցաված է նկ. 2-ում:

**InvShiftRows ձևափոխությունը**

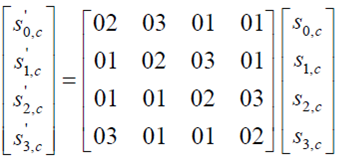
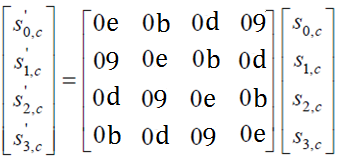
Սա ShiftRows ձևափոխությանը հակադարձ ձևափոխություն է: Վիճակի առաջին տողը մնում է անփոփոխ, երկրորդը 1 բայթով ցիկլիկ տեղաշարժվում է աջ, երրորդը 2 բայթով, չորրորդը՝ 3:

**InvSubBytes ձևափոխությունը**

Սա SubBytes ձևափոխությանը հակադարձ ձևափոխություն է: Բայթերի փոխարինումը իրականացվում է համանմանորեն՝ հակառակ փոխարինումների աղյուսակի համաձայն:

**InvMixColumns ձևափոխությունը**

Սա MixColumns ձևափոխությանը հակադարձ ձևափոխություն է: Վիճակի յուրաքանչյուր սյունյակը ձևափոխվում է առանձին:



InvMixColumns

ձևափոխությունը

MixColumns

ձևափոխությունը

**RSA գաղտնագրային ալգորիթմը**

RSA-ը հանդիսանում է գաղտնագրման առաջին լիակատար անհամաչափ ալգորիթմը, որը կարելի է օգտագործել ինչպես տեղեկատվության գաղտնագրված փոխանակման, այնպես էլ թվային ստորագրության ձևավորման համար և ստեղծվել է 1977թ.: Այն անվանվել է ալգորիթմը մշակոած երեք գիտնականների՝ Ռոն Ռիվեստի (Ron Rivest), Ադի Շամիրիր (Adi Shamir) և Լեոնարդ Էդլմանի (Leonard Adleman) անզգանունների սկզբնատառերով: Գոյություն ունեցող անհամաչափ գաղտնագրային ալգորիթմներից RSA-ն հավանաբար ամենահեշտն է հասկանալու և իրագործելու տեսակետից և միաժամանակ գործնականում ամենատարածվածը: Այս ալգորիթմը երկար տարիներ դիմակայում է ինտենսիվ գաղտնավերլուծությանը: Չնայած գաղտնավերլուծությունը ո՛չ ապացուցել է, ո՛չհակասել RSA-ի ավտանգությունը, այն, ըստ էության, հիմնավորում է ալգորիթմի հանդեպ վստահությունը:

RSA-ի անվտանգությունը հիմնված է մեծ թվերը բազմապատկիչների վերլուծելու բարդության մեջ: Բաց և փակ բանալիները հանդիսանում են երկու մեծ պարզ թվերի ֆունկցիաներ: Ենթադրվում է, որ ըստ գաղտնագրված տեքստի և բաց բանալու, բաց տեքստի վերականգնումը համարժեք է երկու մեծ թվերը բազմապատկիչների վերլուծելուն:

**RSA բանալիների ստացումը**

Երկու բանալիների գեներացման համար օգտագործվում են երկու մեծ պարզ թիվ՝ P և Q: Առավելագույն անվտանգության համար P-ն և Q-ն ընտրվում են միևնույն երկարության: Հաշվում ենք հետևյալ արտադրյալը.

N = P \* Q

Այնուհետև ընտրվում է 1-ից մեծ E թիվ, որը (P-1) \* (Q-1) արտադրյալից փոքր է և փոխադարձաբար պարզ է նրա հետ: N և E թվերը հանդիսանում են բաց բանալին: Վերջում Էվկլիդեսի ընդլայնված ալգորիթմով հաշվվում է D փակ բանալին.

D = E-1 mod ((P-1)(Q-1))

D և N թվերը նույնպես փոխադարձաբար պարզ են: P և Q թվերը այլևս պետք չեն, սակայն պետք է գաղտնի պահվեն, քանի որ նրանց միջոցով կարելի է հաշվարկել D փակ բանալին:

**RSA գաղտնագրում և վերծանում**

M հաղորդագրությունը գաղտնագրելու համար նախևառաջ այն բաժանվում է N-ից փոքր թվային բլոկների (երկուական տվյալների համար ընտրվում է N-ից փոքր 2-ի ամենամեծ աստիճանը): Այսինքն, եթե P-ն և Q-ն 100-կարգանի պարզ թվեր են, ապա N-ը կպարունակի մոտ 200 կարգ և հաղորդագրության յուրաքանչյուր Mi բլոկի երկարությունը պետք է լինի մոտ 200 կարգ: C գաղտնագրված հաղորդագրությունը բաղկացած կլինի միևնույն երկարությամբ Ci բլոկներից: Գաղտնագրման բանաձևն ունի հետևյալ տեսքը՝

ci = mie mod n

Հաղորդագրությունը վերծանելու համար պետք է վերցնել գաղտնագրված Ci բլոկներից յուրաքանչյուրը և հաշվել

mi = cid mod n

Քանի որ

cid = (mie(mod n))d = mied(mod n) = mik(p-1)(q-1)+1(mod n) =

= mi\*mik(p-1)(q-1) (mod n) = mi\*1(mod n) = mi (mod n)

հետևաբար բանաձևը վերականգնում է հաղորդագրությունը:

Նույն կերպ հաղորդագրությունը կարող է գաղտնագրվել D-ի միջոցով և վերծանվել E-ի միջոցով:

**RSA ալգորիթմի արագությունը**

RSA-ի գլխավոր թերությունը կայանում է շատ ցածր արագագործության մեջ: Այդ իսկ պատճառով, մեր խնդրում RSA ալգորիթմով գաղտնագրվում է միայն AES ալգորիթմի բանալին, իսկ տեքստը գաղտնագրվում է AES ալգորիթմով, այսինքն՝ ընդհանուր համակարգի արագագործությունը էականորեն չի տուժում:

RSA ալգորիթմով գաղտնագրում իրականացվում է զգալիորեն ավելի արագ, եթե E-ի արժեքը ճիշտ է ընտրվում: Ամենից հաճախ կիրառվող երեք տարբերակներն են՝ 3, 17 և 65537 (65537 թվեի երկուական ներկայացումները պարունակում է երկու հատ մեկ, ինչի շնորհիվ աստիճան բարձրացնելիս պետք է կատարել ընդամենը 17 բազմապատկում): Այս երեք թվերից ոչ մեկի կիրառության դեպքում չկա անվտանգության խնդիր (այն պայմանով, որ հաղորդագրությունը լրացվում է պատահական թվերով), նույնիսկ եթե E-ն օգտագործվում է օգատագործողների մի ամբողջ խմբի կողմից:

Փակ բանալիներով գործողությունները կարելի արագացնել նաև մնացորդների մասին չինական թեորեմի միջոցով, եթե պահպանվել են P, Q, արժեքները, ինչպես նաև d mod (p - 1), d mod (q - 1) և q-1 mod p լրացուցիչ արժեքները:

**RSA ալգորիթմի անվտանգությունը**

RSA-ի անվտանգությունը ամբողջությամբ կախված է մեծ թվերը բազմապատկիչների վերլուծելու խնդրից: Տեխնիկապես, անվտանգության մասին այս պնդումը կեղծ է: Երբևէ մաթեմատիկորեն չի ապացուցվել, որ ըստ C-ի և E-ի M-ը վերականգնելու համար պետք է N-ը վերլուծել բազմապատկիչների: Հասկանալի է, որ հնարավոր է հայտնաբերվի RSA-ի գաղտնավերլուծության ամբողջովին այլ մեթոդ: Սակայն, եթե այդ մեթոդը օգնի գաղտնավերլուծողին ստանալ D-ն, այն կարող է օգտագործվել նաև մեծ թվերը բազմապատկիչների վերլուծելու ժամանակ:

RSA-ն կարելի է կոտրվել նաև գուշակելով (P-1)(Q-1) արժեքը, ինչն ավելի հեշտ չէ քան N-ը բազմապատկիչների վերլուծելը:

N-ը բազմապատկիչների վերլուծելը կոտրելու ամենաակնհայտ տարբերակն է: Ցանկացած հակառակորդ կարող է ունենալ E բաց բանալին և N մոդուլը: Վերծանման D բանալին գտնելու համար հակառակորդը պետք է N-ը վերլուծի բազմապատկիչների: Ներկա դրությամբ ամենամեծ թիվը, որը վերլուծվել է բազմապատկիչների պարունակում է 129 թվանշան՝ տասական համակարգով: Հետևաբար N-ը պետք է մեծ լինի այդ թվից:

Իհարկե, գաղտնավերլուծողը կարող է փորձել D-ի բոլոր հնարավոր տարբերակները, մինչև գտնի ճիշտ թիվը: Այսպիսի մոտեցումը նվազ արդյունավետ է քան N-ը բազմապատկիչների վերլուծելը:

Ժամանակ առ ժամանակ տարբեր հայտարարաություններ են հայտնվում այն մասին, իբր RSA-ը կոտրելու հեշտ մեթոդը գտնվել է, սակայն դեռևս այդ հայտարարություններից ոչ մեկը չի հաստատվել:

Կա RSA ալգորիթմի անհանգստության համար վստահ լինելու ևս մեկ առիթ: P և Q պարզ թվերի հաշվարկման ալգորիթմների մեծամասնությունը հավանականային են: Իսկ ի՞նչ կլինի, եթե P-ն և Q-ն լինեն բաղադրյալ: Առաջին հերթին կարելի է նման դեպքի հավանականությունը հասցնել նվազագույնի: Եվ նույնիսկ, եթե այդպիսի բան տեղի ունենա, ամենայն հավանականությամբ նմանատիպ դեպքը միանգամից կհայտնաբերվի՝ գաղտնագրումն ու վերծանումը չեն աշխատի: Գոյություն ունեն թվեր, որոնք չեն հայտնաբերվում պարզ թվերի որոմնան հավանականային ալգորիթմների կողմից: Այդ թվերը շատ հազվադեպ են և կոչվում են Կարլմայքլի թվեր: