Հայաստանի Ազգային Պոլիտեխնիկական Համալսարան



Կուրսային Աշխատանք

Առարկա՝ Ծրագրային համակարգերի պաշտպանություն (ԾՀՊ)

Թեմա՝ TwoFish

Խումբ՝ Հ719-2

Ուսանող՝ Աղաջանյան Տիգրան

Դասախոս՝ Արտաշյան Տաթևիկ

ԵՐԵՎԱՆ 2020

***Բովանդակություն***

[*Խնդրի դրվածքը*](#_Toc25700940) *3*

[*Ներածություն*](#_Toc25700941) *3*

[*Ալգորիթմի նկարագրությունը*](#_Toc25700942) *4*

[*Եզրակացություն*](#_Toc25700944) *13*

[*Գրականություն*](#_Toc25700951) *14*

**Խնդրի դրվածքը**

Կոդավորել և ապակոդավորել տեքստը TwoFish կոդավորման ալգորիթմով։

**Ներածություն**

Գաղտնագրության մեջ Twofish- ը սիմետրիկ բլոկային ծածկագրիչ բանալին է, որի բլոկի չափը կազմում է 128 բիթ, իսկ բանալու չափերը ՝ մինչև 256 բիթ: Սա Advanced Encryption Standard ստանդարտ մրցույթի հինգ եզրափակիչ փուլերից մեկն էր, բայց նա չընտրվեց ստանդարտացման համար:

TwoFish- ի տարբերակիչ առանձնահատկություններն են `նախապես հաշվարկված բանալին կախված S- բլոկների օգտագործումը և համեմատաբար բարդ գծապատկերի բանալին: N-bit ստեղնաշարի մեկ կեսը օգտագործվում է որպես կոդավորման փաստացի բանալին, իսկ n-bit ստեղնաշարի մյուս կեսը օգտագործվում է գաղտնագրման ալգորիթմի (բանալին կախված S- տուփերից) փոխելու համար: Twofish- ը փոխառում է որոշ տարրեր այլ ձևավորումներից. Օրինակ ՝ «Adamar» կեղծ վերափոխումը (PHT) `SAFER ծածկագրերի ընտանիքից: Twofish- ը ունի DES- ի նման Feistel- ի կառուցվածք: Twofish- ը նաև օգտագործում է առանձնացված մատրիցաների առավելագույն հեռավորությունը:

\* 128 բիթանոց բլոկային սիմետրիկ ծածկագիր

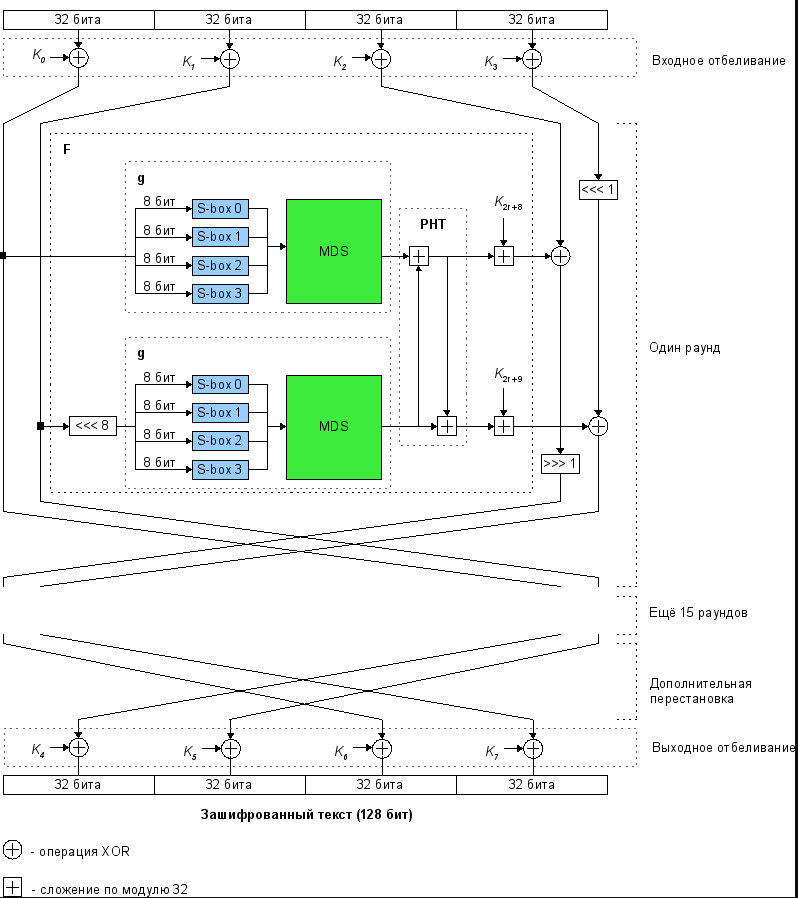
\* Հիմնական երկարությունները 128, 192 և 256 բիթ

\* Թույլ ստեղների բացակայություն

\* Արդյունավետ ծրագրային ապահովում (հիմնականում 32-բիթանոց պրոցեսորների վրա) և ապարատային իրականացում

\* Ալգորիթմի պարզություն `դրա արդյունավետ վերլուծության հնարավորության համար

**Ալգորիթմի նկարագրությունը**



### Отбеливание (whitening)

Սպիտակացնելը Xor- ի տվյալների տակ եղած ենթախմբերի կարգն է առաջին փուլից և վերջին տուրից հետո: Այս տեխնիկան առաջին անգամ օգտագործվել է Խուֆուի / Խարեի ծածկագրերում և, ինքնուրույն, Ռոն Ռիվեստի կողմից DESX կոդավորման ալգորիթմում: Oeո Քիլիան (NEC) և Ֆիլիպ Ռոգավայը (Կալիֆորնիայի համալսարան) ցույց տվեցին, որ սպիտակեցումը իսկապես բարդացնում է DESX- ում սպառիչ ստեղն որոնմամբ բանալին գտնելու առաջադրանքը [3]: Twofish- ի մշակողները պնդում են, որ սպիտակեցումը նաև էապես բարդացնում է Twofish- ում առանցքային ընտրության առաջադրանքը, քանի որ ծպտյալ վերլուծաբանը չի կարող պարզել, թե որ տվյալներն են անցնում առաջին փուլի F գործառույթի մուտքագրմանը:

### Функция g

G ֆունկցիան Twofish ալգորիթմի հիմքն է: Ֆունկցիայի մուտքը 32 բիթանոց թիվ է, այնուհետև բաժանվում է չորս բայթ ՝ x0, x1, x2, x3: Արդյունքում ստացված բայթերից յուրաքանչյուրն անցնում է իր S- տուփով: (Պետք է նշել, որ ալգորիթմի S տուփերի ամրագրերը ամրագրված չեն, բայց կախված են բանալին): Արդյունքում ստացված 4 բայթը S-box- ի թողարկումներում մեկնաբանվում է որպես չորս բաղադրիչ ունեցող վեկտոր: Այս վեկտորը բազմապատկվում է ֆիքսված 4x4 MDS (առավելագույն հեռավորության տարանջատող) մատրիցով, իսկ հաշվարկներն իրականացվում են Galois դաշտում GF (2 ^ 8) մոդուլով ՝ անխորտակելի բազմագույնը 

MDS- ի մատրիցան այնպիսի մատրիցա է, որը պատկանում է վերջավոր դաշտի K- ին, եթե այն վերցնում ենք որպես գծային փոխակերպման մատրիցա f(x) = (MDS)x տարածությունից K ^ n տարածության մեջ K^m, ապա տիեզերքից ցանկացած երկու վեկտոր K ^ (n + m) ձևի (x, f (x)) բաղադրիչները կունենան առնվազն m + 1 տարբերություններ: Այսինքն, ձևի վեկտորների մի շարք (x, f (x)) կազմում է կոդ, որն ունի առավելագույն հեռավորության բաժանվող կոդի հատկությունը: Այսպիսի ծածկագիրը, օրինակ, Ռիդ-Սողոմոնի ծածկագիրն է:

Twofish- ում MDS մատրիցի առավելագույն բազմազանությունը նշանակում է, որ վեկտորի a և վեկտորի փոփոխվող բայթերի ընդհանուր քանակը b = (MDS)a- ն առնվազն հինգ է: Այլ կերպ ասած, a- ի միայն մեկ բայթում ցանկացած փոփոխություն հանգեցնում է b- ի բոլոր չորս բայթերի փոփոխությանը:

### Pseudo-Hadamar Transform (PHT)

Hadamard կրիպտո փոխարկումը 2n հետադարձելի բիթային լարային փոխարկում է: Տողը բաժանվում է n բիթերի նույն երկարության a և b մասերի երկու մասի: Փոխարկումը հաշվարկվում է հետևյալ կերպ.



Այս գործողությունը հաճախ օգտագործվում է ծածկագիրը ծածկելու համար (օրինակ ՝ SAFER ծածկագրում):

Twofish- ում այս փոխակերպումն օգտագործվում է երկու g- ֆունկցիաների արդյունքները խառնելիս (n = 32):

### Циклический сдвиг на 1 бит

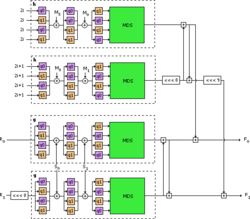
### Յուրաքանչյուր փուլում F- ի գործառույթի արդյունքներով փչացող երկու ճիշտ 32 բիթանոց բլոկները լրացուցիչ ցիկլիկորեն տեղափոխվում են մեկ բիտով: Երրորդ բլոկը տեղափոխվում է xor- ի շահագործումից առաջ, չորրորդ բլոկը `դրանից հետո: Այս տեղաշարժերը հատուկ ավելացվել են բայթ բայթերի հավասարեցումը խախտելու համար, որոնք բնորոշ են S- տուփերին և MDS մատրիցով բազմապատկման գործողություններին: Այնուամենայնիվ, կոդավորումը դադարում է ամբողջովին սիմետրիկ լինել, քանի որ գաղտնագրման և գաղտնագրման ընթացքում տեղաշարժերը պետք է իրականացվեն հակառակ ուղղությամբ:

### Генерация ключей

## Twofish- ը նախատեսված է 128, 192 և 256 բիթ երկարությունների բանալիների հետ աշխատելու համար: Բուն ստեղնից ստացվում են 40 32 բիթանոց ենթախցիկներ, որոնցից առաջին ութը օգտագործվում են միայն մուտքային և ելքային սպիտակեցման գործողություններում, իսկ մնացած 32-ը օգտագործվում են կոդավորման փուլերում ՝ երկու ենթափայտ յուրաքանչյուր փուլ: Twofish- ի առանձնահատկությունն այն է, որ աղբյուրի ստեղնը նույնպես օգտագործվում է կոդավորման ալգորիթմը ինքնին փոխելու համար, քանի որ g գործառույթներում օգտագործված S- արկղերը ամրագրված չեն, բայց կախված են ստեղնից:

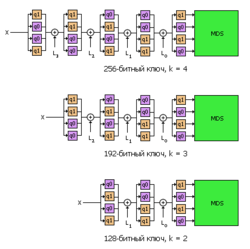
## Կլոր ենթախցիկներ ձևավորելու համար M- ի սկզբնական բանալին բաժանվում է բայթերի վերադասավորմամբ ՝ երկու նույնական բլոկ և: Այնուհետև, օգտագործելով բլոկը և գործառույթը h, 2 \* i արժեքը կոդավորված է, և բլոկը օգտագործելով ՝ 2 \* i + 1 արժեքը կոդավորված է, որտեղ i- ն ընթացիկ փուլի թիվն է (0 - 15): Արդյունքում կոդավորված բլոկները խառնվում են Hadamard ծպտյալ փոխակերպման միջոցով, այնուհետև օգտագործվում են որպես կլոր ենթախցիկներ:

## Технические подробности

[](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Twofish_round.png)Схема одного раунда шифрования для 128-битного ключа

Եկեք ավելի մանրամասն քննարկենք կլոր ենթախցերի առաջացման ալգորիթմը, ինչպես նաև բանալին կախված գործառույթը g. Թե՛ ենթակապերի ձևավորման, և g գործառույթի ձևավորման համար Twofish- ը օգտագործում է մեկ հիմնական գործառույթ ՝ h (X, L0, L1, ..., Lk): Այստեղ X, L0, L1, ..., Lk- ն 32 բիթ բառ է, իսկ k = N / 64, որտեղ N- ը բիթային բանալիի երկարությունն է բիթերով: Գործառույթի արդյունքը մեկ 32 բիտանոց բառ է:

Функция h

[](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Twofish_h_func.png)

Функция h для разных длин ключа

Գործառույթը կատարվում է k փուլերով: Այսինքն, ստեղնաշարի 256 բիթանոց երկարության համար կլինի 4 փուլ, 192-բիթանոց ստեղնի համար `3 փուլ, 128 բիթի համար` 2 փուլ:

Յուրաքանչյուր փուլում մուտքային 32-բիթ բառը բաժանվում է 4 բայթ, և յուրաքանչյուր բայթ անցնում է q0 կամ q1 բիթերի ֆիքսված пермутација:

Արդյունքը ներկայացված է որպես 4 բայթ բեռի վեկտոր և բազմապատկվում է MDS մատրիցով: Հաշվարկներն իրականացվում են Galois դաշտում GF (28) մոդուլում ՝ անխորտակելի բազմակնություն:

Q0 և q1 q0 և q1 permutations- ը մուտքային բայթ x- ի 8 բիթերի ֆիքսված պերվուտացիաներ են:

Բայթ x- ը բաժանվում է երկու 4 բիթանոց կեսերի a0 և b0, որոնց վրա կատարվում են հետևյալ վերափոխումները.

Ահա 4-բիթանոց ցիկլային հերթափոխը դեպի աջ, և t0, t1, t2, t3- ը 4-բիտ համարների աղյուսակային փոխարինումներ են

Q0- ի համար աղյուսակները ձևի են.

t0 = [8 1 7 D 6 F 3 2 0 B 5 9 E C A 4]

t1 = [E C B 8 1 2 3 5 F 4 A 6 7 0 9 D]

t2 = [B A 5 E 6 D 9 0 C 8 F 3 2 4 7 1]

t3 = [D 7 F 4 1 2 6 E 9 B 3 0 8 5 C A]

Q1- ի համար աղյուսակները ձևի են.

t0 = [2 8 B D F 7 6 E 3 1 9 4 0 A C 5]

t1 = [1 E 2 B 4 C 3 7 6 D A 5 F 9 0 8]

t2 = [4 C 7 5 1 6 9 A 0 E D 8 2 B 3 F]

t3 = [B 9 5 1 C 3 D E 6 4 7 F 2 0 8 A]

Генерация ключей

Թող M- ը լինի աղբյուրի բանալին, N- ը դրա բիթերի երկարությունն է: Ենթաբաժինների սերունդը հետևյալն է.

Բուն ստեղնը բաժանված է 8 \* k բայթ

 {\displaystyle m\_{0},...,m\_{8k-1}}  

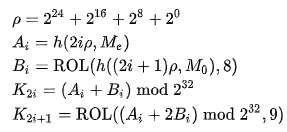
Այս 8 \* կ բայթերը բաժանվում են չորս բայթ բառերի, և յուրաքանչյուր բառում բայթերը վերադասավորվում են հակառակ հերթականությամբ: Արդյունքը 2 \* k 32 բիթանոց բառ է Mi



Արդյունքում ստացված 2 \* k 32 բիթանոց բառերը բաժանվում են երկու վեկտորների ՝ k 32-bit բառերի չափը:



I- րդ փուլի միացումները հաշվարկվում են բանաձևերով.

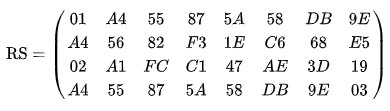


### Функция g и S-box’ы

Գործառույթը g սահմանվում է h գործառույթի միջոցով. g(X) = հ(X, S)

Վեկտորը S- ը, ինչպես վեկտորները Me, Mo- ն, նույնպես ձևավորվում են բնօրինակ բանալուց և բաղկացած է k 32-bit բառերից: Բանալու բուն բայթերը բաժանվում են ութ բայթ ունեցող k խմբերի: Յուրաքանչյուր նման խումբ համարվում է որպես 8 բաղադրիչ ունեցող վեկտոր և բազմապատկվում է ֆիքսված RS մատրիցով `4x8 բայթ չափսերով: Բազմապատկման արդյունքում ձեռք է բերվում չորս բայթից բաղկացած վեկտոր: Հաշվարկներն իրականացվում են Galois դաշտում displaystyle GF (2^8) modulo irreducible polynomial 

RS- մատրիցը ունի ձև.

****

{\displaystyle K\_{2i}=(A\_{i}+B\_{i}){\bmod {2^{32}}}}

{\displaystyle K\_{2i+1}={\mbox{ROL}}((A\_{i}+2B\_{i}){\bmod {2^{32}}},9)}

**Եզրակացություն**

Աշխատանքի արդյունքում ավելի պարզ արտահայտվեց այն փաստը,որ մի բլոկի փոփոխությունը մեծ ազդեցություն է ունենում մյուս բլոկների վրա ,ինչպես նաև վերջնական արդյունքը սխալ է ստացվում։ Չնայած այն համարվում է սիմետրիկ բանալիով ալգորիթմ ,սակայն իր բազմազան ֆունկցիաների շնորհիվ դառնում է հուսալի ալգորիթմ։

**Գրականություն**

<https://github.com/>

<https://ru.wikipedia.org/wiki/Twofish>