# METODE CRIPTOGRAFICE DE PROTECȚIE A INFORMAȚIEI

## Tema: Cifruri bloc moderne

# SISTEMUL DE CRIPTARE AES

Actualmente, sistemul de criptare AES (Advanced Encryption Standard) este cel mai popular cifru bloc cu cheie simetrică, utilizat într-un număr mare de sisteme comerciale. Printre standardele comerciale ce includ AES vom menționa standardul de securitate Internet IPsec, protocolul pentru comunicații pe Internet TLS, standardul de criptare Wi-Fi IEEE 802.11i, protocolul de rețea SSH (Secure Shell) și telefonia prin Internet Skype. Până în prezent nu au fost elaborate atacuri criptanalitice asupra AES mai eficiente ca atacul prin forță brută.

# SISTEMUL DE CRIPTARE AES

Obiectivele de bază ale secțiunii sunt următoarele:

- A prezenta etapele proiectării standardului de criptare AES;
- A examina structura generală a algoritmilor de criptare și de decriptare AES;
- A analiza transformările utilizate în cadrul sistemului de criptare AES (substituția de octeți, difuzia, mixarea cheii, expandarea cheii);
- A descrie operații definite pe mulțimi ce formează corpuri Galois – structuri algebrice pe care este bazată securitatea AES;
- A analiza eficiența implementărilor AES.

### *2.3.5.1 Finalistele la concursul pentru AES*

Deoarece DES devenise vulnerabil din cauza lungimii prea mici a cheii, NIST (National Institute of Standards and Technology of the United States) a recomandat utilizarea 3DES. Sistemul de criptare 3DES s-a dovedit a fi un algoritm cu o rezistență criptografică înaltă, dar lent în implementările software și hardware (chiar nepotrivit pentru platformele cu resurse limitate), motiv pentru care NIST a lansat la 2 ianuarie 1997 un concurs pentru desemnarea unui algoritm care să înlocuiască DES. S-a ales și numele noului sistem de criptare - AES (Advanced Encryption Standard).

# SISTEMUL DE CRIPTARE AES

La fel, NIST a specificat criteriile pe care urma să le satisfacă noul sistem de criptare:

- Să fie un sistem de criptare simetrică bloc public accesibil (freeware).
- Să aibă lungimea blocului de 128 biți.
- Să accepte chei de lungime 128, 192 și 256 biți.
- Să nu se conțină chei slabe în spațiul de chei.
- Să fie eficient atât pe platforme Intel Pentium Pro, cât și pe alte platforme software sau hardware.
- Să poată fi implementat atât pe sisteme cu procesoare pe 32 biți (actuale la acel moment), cât și pe sisteme cu procesoare pe 8 biți (smart-carduri).
- Să fie cât mai simplu posibil.
- Să fie mai rapid decât DES, iar rezistența criptografică a acestuia să nu fie mai mică ca cea pentru 3DES.

# SISTEMUL DE CRIPTARE AES

Inițial au fost acceptați 21 de algoritmi propuși de membri ai comunității criptografice mondiale. După prima conferință pentru selectarea candidaților AES, organizată de NIST, au fost selectați 15 candidați care satisfăceau specificărilor formulate. În ordine alfabetică aceste cifruri sunt următoarele: CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, Rijndael, SAFER+, Serpent, Twofish. În cadrul unor dezbateri au fost stabilite mai multe avantaje și dezavantaje ale candidaților. NIST a organizat două conferințe (AES1 în august 1998 și AES2 în martie 1999) în cadrul cărora au fost discutați candidații propuși, iar în august 1999 a anunțat cinci finaliști ai concursului pentru AES: Mars, RC6, Rijndael, Serpent, Twofish.

În Tabelul 2.3.10 este prezentată repartizarea voturilor pentru cei cinci finaliști:

| Algoritm | Voturi pro | Voturi contra |
|---|---|---|
| Rijndael | 86 | 10 |
| Serpent | 59 | 7 |
| Twofish | 31 | 21 |
| RC6 | 23 | 37 |
| Mars | 13 | 84 |

*Tabelul 2.3.10. Repartizarea voturilor pentru finaliștii AES*

Criteriile în baza cărora au fost evaluați algoritmii sunt următoarele: securitatea (rezistența la atacuri criptanalitice), costul (eficiența computațională, spațiul de memorie utilizat, precum și licența liberă și gratuită) și particularitățile algoritmului (flexibilitatea realizării pe orice platformă, simplitatea realizării implementărilor software și hardware).

# SISTEMUL DE CRIPTARE AES

În aprilie 2000 s-a desfășurat conferința AES3 în cadrul căreia reprezentanții echipelor care au elaborat cei cinci algoritmi au adus argumente în favoarea sistemului de criptare pe care îl reprezintă. La 2 octombrie 2000 NIST a anunțat că învingătorul concursului pentru AES este algoritmul Rijndael (elaborat de doi criptografi belgieni, J. Daemen și V. Rijmen). Astfel, la 26 noiembrie 2001 algoritmul Rijndael devine oficial AES, noul standard de criptare aprobat de NIST în cadrul FIPS PUB 197. AES a fost selectat în cadrul unui concurs deschis, care s-a desfășurat în mod transparent, spre deosebire de modul în care a fost aprobat predecesorul său DES. La fel, AES a fost inclus în standardul ISO/IEC 18033-3.

# SISTEMUL DE CRIPTARE AES

***Detalii ale sistemului de criptare AES***

Cifrul bloc AES (Advanced Encryption Standard) este cunoscut și sub numele de Rijndael. Familia de algoritmi Rijndael este caracterizată prin chei și blocuri de lungime variabilă în biți ce reprezintă un multiplu al lui 32, cu valori între 128 și 256 biți.

De fapt, AES este format dintr-o submulțime de trei algoritmi ai familiei Rijndael, cu lungimea cheii secrete, respectiv, de 128, 192 și 256 biți și lungimea de bloc fixată la 128 biți pentru fiecare (a se vedea Figura 2.3.17).

Strategia utilizată în construcția cifrului bloc AES (Rijndael) constă în divizarea funcției de rundă pe componente cu funcționalitate distinctă, care asigură rezistență în fața atacurilor criptanalitice. Această metodă de proiectare a funcțiilor de rundă este bazată pe strategia Wide Trail

# SISTEMUL DE CRIPTARE AES

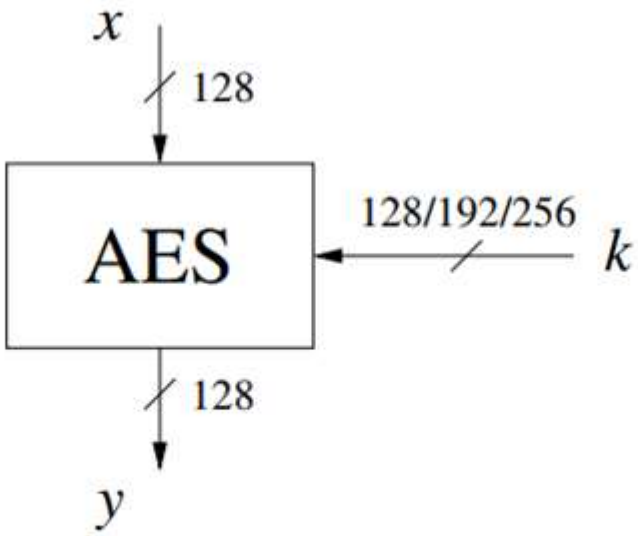


*Figura 2.3.17. Schema generală pentru algoritmul de criptare AES*

### *2.3.5.2.1 Elemente teoretice folosite în implementarea algoritmului AES*

Mai întâi vom prezenta aspectele matematice necesare pentru descrierea sistemului de criptare AES.

#### *2.3.5.2.1.1 Corpul finit*

Majoritatea calculelor în cadrul algoritmului AES sunt operații efectuate cu elementele unui corp finit (numit și corp Galois).

Înainte de a defini noțiunea de corp este necesar să amintim conceptul mai simplu al structurii algebrice numite grup.

# SISTEMUL DE CRIPTARE AES

*Definiția 2.3.1. Grupul este o mulțime de elemente* $G$ *peste care este definită o operație „*$\circ$*” ce combină două elemente ale lui* $G$ *astfel încât să se satisfacă proprietățile:*

1. *Operația* $\circ$ *este închisă, adică pentru orice* $a,b \in G$ *avem* $a \circ b = c \in G$;
2. *Operația* $\circ$ *este asociativă, adică pentru orice* $a,b,c \in G$ *avem* $a \circ (b \circ c) = (a \circ b) \circ c$;
3. *Există un element în* $G$, *notat prin* $1$ *și numit element neutru, pentru care se satisface condiția* $a \circ 1 = 1 \circ a = a$ *pentru orice* $a \in G$;
4. *Pentru fiecare* $a \in G$ *există un element* $a^{-1} \in G$, *numit invers al lui* $a$, *astfel încât* $a \circ a^{-1} = a^{-1} \circ a = 1$.

*Definiția 2.3.2. Grupul $G$ este comutativ (sau abelian) dacă se satisface condiția* $a \circ b = b \circ a$ pentru orice $a, b \in G$.

Dacă operația ce definește structura de grup este adunarea, atunci operația inversă este diferența, iar dacă operația este înmulțirea, atunci operația inversă – înmulțirea cu elementul invers.

***Exemplul 2.3.4.*** Mulțimea claselor de resturi modulo $m$, $\mathbb{Z}_m = \{0,1,\ldots,m-1\}$, peste care este definită operația „+" de adunare modulo $m$, formează un grup cu elementul neutru $0$. Fiecărui element $a \in \mathbb{Z}_m$ îi corespunde un invers aditiv $(-a)$ pentru care se satisface condiția $\mathrm{mod}\left(a+(-a), m\right) = 0$. De menționat că $\mathbb{Z}_m$ nu formează un grup în raport cu operația „$\cdot$" de înmulțire modulo $m$, deoarece sunt mai multe elemente $a \in \mathbb{Z}_m$ care nu admit un invers ce satisface condiția $\mathrm{mod}\left(aa^{-1}, m\right) = 1$. □

# SISTEMUL DE CRIPTARE AES

Pentru ca o structură matematică să fie definită în baza celor patru operații aritmetice (adunarea, scăderea, înmulțirea și împărțirea), se definește o mulțime ce conține două grupuri în raport cu aceste operații: unul aditiv și altul multiplicativ. Corpul este structura algebrică definită în baza a două operații: adunarea „+” și înmulțirea „*”.

*Definiția 2.3.3. Corpul este o mulțime de elemente* $\mathcal{K}$ *peste care sunt definite operațiile de adunare „+ ” și înmulțire „* $*$ *”, în raport cu care se satisfac condițiile:*

- *Mulțimea* $\mathcal{K}$ *formează un grup aditiv comutativ în raport cu operația de adunare* $+$*. Elementul neutru al acestui grup aditiv este notat prin* $0 \in \mathcal{K}$*, iar inversul aditiv al elementului* $a \in \mathcal{K}$ *- prin* $(-a) \in \mathcal{K}$*.*
- *Mulțimea* $\mathcal{K}$*, din care se exclude elementul nul* $0$*, formează un grup multiplicativ comutativ în raport cu operația de înmulțire* $*$*. Elementul neutru al acestui grup este notat prin* $1 \in \mathcal{K}$*, iar inversul multiplicativ al elementului* $a \in \mathcal{K}$ *- prin* $a^{-1} \in \mathcal{K}$*. Elementul* $0 \in \mathcal{K}$ *nu este inversabil în raport cu operația de înmulțire* $*$*.*
- *Pentru orice elemente* $a, b, c \in \mathcal{K}$ *se satisface următoarea lege distributivă:*

$$a * (b + c) = (a * b) + (a * c).$$

# SISTEMUL DE CRIPTARE AES

Există structuri matematice de corp cu un număr infinit de elemente, cum ar fi, corpul numerelor reale $\mathbb{R}$ sau corpul numerelor complexe $\mathbb{C}$. Însă în cadrul criptografiei sunt examinate mulțimi cu un număr finit de elemente ce formează structură de corp (numit corp finit sau corp Galois). Acestea se definesc astfel: pentru orice număr prim $p$ și număr întreg $n \geq 1$, există o singură mulțime din $p^n$ elemente, notată prin $GF\left(p^n\right)$, care formează o structură matematică de corp. Faptul că un corp finit este unic înseamnă că oricare două corpuri cu același număr de elemente, diferă doar prin „numele" elementelor.

# SISTEMUL DE CRIPTARE AES

În cazul în care $n=1$, corpul finit $GF(p)$ este format din numerele întregi modulo $p$, iar operațiile de adunare și înmulțire definite peste acesta sunt, respectiv, adunarea modulo $p$ și înmulțirea modulo $p$, a două numere întregi. Elementele nenule ale lui $GF(p)$ admit invers multiplicativ. Astfel, pentru un element nenul $a \in \mathbb{Z}_p$, se determină elementul invers $a^{-1} \in \mathbb{Z}_p$ ce satisface condiția $\mathrm{mod}(a * a^{-1}, p) = 1$. Calculul inversului multiplicativ se poate realiza în baza algoritmului Euclid extins. Un caz particular îl reprezintă corpul $GF(2)$, în care adunarea este operația XOR, iar înmulțirea – operația AND.

Valoarea $p^n$ definește numărul de elemente ale corpului, iar valoarea $p$ este numită caracteristică a corpului.

*2.3.5.2.1.2 Operații definite peste corpul finit GF($2^8$)*

Operațiile AES sunt definite la nivel de octeți, care sunt considerați ca elemente ale corpului finit $GF\left(2^8\right)$. Alte operații sunt definite la nivel de cuvinte pe 4 octeți (32 biți).

Corpul Galois $GF\left(2^8\right)$ ( $p=2, n=8$ ) conține numere reprezentabile pe un octet. Întrucât cel mai mare număr întreg reprezentabil pe un octet este

$$\left(11111111\right)_2 = 2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0 = 255,$$

se operează cu numere întregi din intervalul $\left[0,255\right]$. Deoarece există 256 de simboluri în codul ASCII, se poate asocia în mod unic fiecare simbol unui element din $GF\left(2^8\right)$.

# SISTEMUL DE CRIPTARE AES

Deoarece ordinul corpului finit $GF\left(2^8\right)$ nu este un număr prim ($2^8 = 256$ nu este un număr prim), operațiile de adunare și de înmulțire în $GF\left(2^8\right)$ nu pot fi reprezentate prin adunarea și înmulțirea întregilor modulo $2^8$. Astfel, se va utiliza o altă reprezentare pentru elementele corpului $GF\left(2^8\right)$ și se vor defini alte operații asupra acestora.

# SISTEMUL DE CRIPTARE AES

Elementele unui corp finit pot fi reprezentate în diverse moduri. Deoarece $GF\left(2^8\right)$ este unicul corp finit de ordinul 256, toate reprezentările lui $GF\left(2^8\right)$ sunt izomorfe. Cu toate acestea, modul de reprezentare a elementelor influențează complexitatea de implementare. În algoritmul AES se optează pentru reprezentarea polinomială a elementelor lui $GF\left(2^8\right)$. Astfel, octetul $b = b_7 b_6 ... b_0$ (biții sunt scriși de la dreapta spre stânga) nu se va reprezenta ca un întreg, ci ca un polinom $b_7 x^7 + b_6 x^6 + ... + b_1 x + b_0$ cu coeficienți binari $b_i \in GF\left(2\right) = \left\{0,1\right\}$. Reciproc, fiecare polinom cu coeficienți binari poate fi memorat ca un vector cu 8 elemente biți: $\bar{b} = \left(b_7, b_6, ..., b_0\right)$.

Polinoamele au gradul maximal 7, iar cei 8 coeficienți ai acestora definesc elementul din $GF\left(2^8\right)$. De menționat că există 256 de polinoame cu coeficienți binari de grad maximal 7. Mulțimea formată din aceste 256 de polinoame constituie corpul Galois $GF\left(2^8\right)$.

*2.3.5.2.1.3 Notații pentru octeți și biți*

Datele de intrare și de ieșire, precum și cheia secretă sunt șiruri de octeți. În algoritmul AES biții octetului sunt indexați în ordinea $\{b_7, b_6, ..., b_1, b_0\}$. Octetul este interpretat ca element al corpului finit $GF\left(2^8\right)$ în baza reprezentării polinomiale $\sum_{i=0}^{7} b_i x^i$. De exemplu, octetul $(01100011)_2$ specifică elementul $x^6 + x^5 + x + 1$.

# SISTEMUL DE CRIPTARE AES

Unele operații în aritmetica corpului finit $GF\left(2^8\right)$ implică un bit adițional $b_8$, care se scrie la stânga octetului. În hexazecimal vom nota acest bit adițional prin $\{01\}_{16}$. De exemplu, un șir de 9 biți se va scrie sub forma $\{01\}_{16}\{1b\}_{16}$.

Pentru șirul de 128 biți $input_0 input_1 ... input_{127}$ vom considera tablouri de octeți, care se vor scrie sub forma $a_0 a_1 ... a_{15}$, unde

$$a_0 = \{input_0, input_1, ..., input_7\},\ a_1 = \{input_8, input_9, ..., input_{15}\}, ..., a_{15} = \{input_{120}, input_{121}, ..., input_{127}\}.$$

Regula se extinde și pentru șiruri de lungime mai mare, astfel încât avem (a se vedea *Tabelul 2.3.11*)

$$a_n = \{input_{8n}, input_{8n+1}, ..., input_{8n+7}\}.$$

| Șirul de biți | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Indexare octet | 0 | | | | | | | | 1 | | | | | | | | 2 | | | | | | | | ... |
| Indexare biți în cadrul octetului | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | ... |

*Tabelul 2.3.11. Indicii utilizați pentru octeți și biți*

Elementele corpului finit $GF\left(2^8\right)$ pot fi adunate și înmulțite, dar aceste operații diferă de cele utilizate pentru întregi.

*2.3.5.2.1.3.1 Adunarea elementelor din GF($2^8$)*

Adunarea a două elemente ale corpului finit $GF\left(2^8\right)$ este un polinom ai cărui coeficienți sunt obținuți prin adunarea modulo 2 (operația XOR) a coeficienților puterilor corespunzătoare ale polinoamelor asociate celor două elemente.

Deoarece fiecare element $b \in GF\left(2^8\right)$ coincide cu inversul său aditiv $\left(-b\right)$, diferența $a-b$ de elemente din $GF\left(2^8\right)$ coincide cu adunarea acestora, $a-b=a+\left(-b\right)=a+b$.

# SISTEMUL DE CRIPTARE AES

Astfel, suma $a(x)+b(x)$ și diferența $a(x)-b(x)$ a elementelor $a(x),b(x)\in GF\left(2^8\right)$, reprezentate sub formă polinomială $a(x)=\sum_{i=0}^{7}a_i x^i$, $b(x)=\sum_{i=0}^{7}b_i x^i$, se calculează în baza aceleiași relații:

$$c(x)=a(x)\pm b(x)=\sum_{i=0}^{7}c_i x^i,\ c_i\equiv \mathrm{mod}(a_i+b_i,2)=a_i\oplus b_i.$$

# SISTEMUL DE CRIPTARE AES

Prin urmare, adunarea elementelor corpului finit $GF\left(2^8\right)$ poate fi reprezentată ca XOR-ul biților corespunzători ai octeților asociați. Pentru doi octeți $\{a_7a_6a_5a_4a_3a_2a_1a_0\}$ și $\{b_7b_6b_5b_4b_3b_2b_1b_0\}$, suma $\{c_7c_6c_5c_4c_3c_2c_1c_0\}$ se determină prin relația $c_i = a_i \oplus b_i,\ i = \overline{7,0}$. Următoarele relații sunt echivalente:

$$\left(x^6 + x^4 + x^2 + x + 1\right) + \left(x^7 + x + 1\right) = x^7 + x^6 + x^4 + x^2 \text{ (notație polinomială);}$$

$$\left(01010111\right)_2 \oplus \left(10000011\right)_2 = \left(11010100\right)_2 \text{ (notație în binar);}$$

$$\{57\}_{16} \oplus \{83\}_{16} = \{d4\}_{16} \text{ (notație în hexazecimal).}$$

Mixarea cheii din cadrul AES folosește operația de însumare a elementelor din $GF\left(2^8\right)$.

*2.3.5.2.1.3.2 Înmulțirea elementelor din GF(2⁸)*

Înmulțirea elementelor din $GF\left(2^8\right)$ reprezintă operația de bază a transformării *MixColumn* din cadrul AES.

În reprezentare polinomială, înmulțirea a două elemente din $GF\left(2^8\right)$ (notată prin „$\cdot$”) corespunde înmulțirii standard a polinoamelor asociate elementelor, modulo un polinom ireductibil de gradul 8, cu coeficienți binari. Un polinom este ireductibil dacă unicii divizori ai acestuia sunt constanta 1 și el însuși, adică acesta nu poate fi reprezentat ca produs de două polinoame de grad mai mic. Pentru algoritmul AES polinomul ireductibil este $m(x)=x^8+x^4+x^3+x+1$ sau $\{01\}_{16}\{1b\}_{16}$ în notație hexazecimală. Avem

$$c'(x):=a(x)b(x)=\left(a_7x^7+\ldots+a_0\right)\left(b_7x^7+\ldots+b_0\right),$$

$$c'(x) = c'_{14}x^{14} + \ldots + c'_0,$$

unde

$$c'_0 = \mathrm{mod}(a_0 b_0, 2),\ c'_1 = \mathrm{mod}(a_0 b_1 + a_1 b_0, 2), \ldots,\ c'_{14} = \mathrm{mod}(a_7 b_7, 2).$$

De menționat că toți coeficienții $a_i, b_i$ și $c'_i$ sunt elemente din $GF(2)$, prin urmare, calculele sunt efectuate, folosind operațiile definite pe $GF(2)$. Polinomul $c'(x)$ poate să fie de grad mai mare ca 7 și, de aceea, urmează să fie redus. Reducerea are loc prin calculul restului împărțirii polinomului $a(x)b(x)$ prin polinomul ireductibil $m(x) = \sum_{i=0}^{8} p_i x^i,\ p_i \in GF(2)$:

$$c(x) \equiv \mathrm{mod}(a(x)b(x), m(x)).$$

# SISTEMUL DE CRIPTARE AES

Rezultatul reducției modulare prin $m(x)$ este un polinom cu coeficienți binari de grad mai mic ca 8 și, prin urmare, acesta poate fi reprezentat ca un octet. Spre deosebire de adunare, nu există o operație simplă la nivel de octet care să corespundă acestei înmulțiri.

***Exemplul 2.3.5.*** Vom înmulți elementele $\{57\}_{16}$ și $\{83\}_{16}$ din $GF\left(2^8\right)$. Deoarece $\{57\}_{16}=(01010111)_2$, $\{83\}_{16}=(10000011)_2$, avem reprezentările polinomiale $a(x):=x^6+x^4+x^2+x+1$, $b(x):=x^7+x+1$.

Înmulțim polinoamele $a(x)$ și $b(x)$, ținând cont că în polinomul rezultat $c(x)$ coeficienții sunt elemente din $GF(2)$:

$$c(x)=a(x)b(x)=\left(x^6+x^4+x^2+x+1\right)\left(x^7+x+1\right)=$$

$$x^{13}+x^{11}+x^9+x^8+x^7+x^7+x^5+x^3+x^2+x+x^6+x^4+x^2+x+1=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1.$$

Determinăm restul împărțirii polinomului $c(x)$ la polinomul ireductibil $m(x)=x^8+x^4+x^3+x+1$:

$$\mathrm{mod}\left(x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1,x^8+x^4+x^3+x+1\right)=x^7+x^6+1.$$

În rezultat, se obține $(11000001)_2=\{c1\}_{16}$. Astfel, avem $\{57\}_{16}\cdot\{83\}_{16}=\{c1\}_{16}$. □

*2.3.5.2.1.3.3 Inversul multiplicativ în GF(2⁸)*

Calculul inversului multiplicativ în $GF\left(2^8\right)$ reprezintă operația de bază a transformării *Byte Substitution* din cadrul AES.

Elementul $a^{-1} \in GF\left(2^m\right)$ este numit invers multiplicativ al elementului nenul $a \in GF\left(2^m\right)$, dacă reprezentările polinomiale $a^{-1}(x)$ și, respectiv, $a(x)$ pentru aceste elemente satisfac condiția

$$\mathrm{mod}\left(a^{-1}(x)a(x), \tilde{m}(x)\right) = 1,$$

unde $\tilde{m}(x)$ este un polinom ireductibil.

Înmulțirea elementelor din $GF\left(2^8\right)$, definită la secțiunea anterioară, este asociativă, iar elementul $\{01\}_{16}$ este elementul neutru multiplicativ.

# SISTEMUL DE CRIPTARE AES

Inversul multiplicativ al elementului $a \in GF\left(2^m\right)$ poate fi calculat în mai multe moduri:

- Se înmulțește elementul $a \in GF\left(2^m\right)$ cu fiecare element al corpului până se obține elementul neutru multiplicativ $\{01\}_{16}$. Această abordare poate fi considerată ca o căutare prin forță brută.
- Deoarece elementele nenule ale lui $GF\left(2^m\right)$ formează un grup finit în raport cu operația de înmulțire, avem $a^{2^m-1} = 1 \left(a \neq 0\right)$, și atunci inversul $a^{-1}$ este $a^{2^m-2}$.

# SISTEMUL DE CRIPTARE AES

- Pentru orice polinom nenul cu coeficienți binari $b(x)$, de grad mai mic sau egal ca 7, inversul multiplicativ al lui $b(x)$ poate fi stabilit în modul următor: folosind algoritmul Euclid extins ( [13], p. 81-83) se determină polinoamele $a(x)$ și $c(x)$ ce satisfac condiția $b(x)a(x)+m(x)c(x)=1$. Atunci, pentru polinoamele $a(x)$ și $b(x)$ se satisfice condiția $\mathrm{mod}(a(x)b(x),m(x))=1$, ceea ce înseamnă că $b^{-1}(x)=\mathrm{mod}(a(x),m(x))$.

# SISTEMUL DE CRIPTARE AES

Dacă mulțimea ce definește structura de corp conține un număr mic de elemente (nu mai mult de $2^{16}$ elemente), atunci pentru determinarea inverselor multiplicative a elementelor sunt folosite tabele cu inversele precalculate. În Tabelul 2.3.12 sunt prezentate inversele tuturor elementelor din $GF\left(2^8\right)$ modulo polinomul ireductibil $m(x)=x^8+x^4+x^3+x+1$. Aceste valori în reprezentare hexazecimală sunt utilizate în cadrul S-boxei AES. Deși pentru elementul nul nu există un invers multiplicativ, în Tabelul 2.3.12 octetul $\{00\}_{16}$ este aplicat în $\{00\}_{16}$. Acest lucru este făcut din considerentul că S-boxa AES necesită valori de ieșire pentru orice valoare de intrare.

# SISTEMUL DE CRIPTARE AES

| | | y | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
| x | 0 | 00 | 01 | 8d | f6 | cb | 52 | 7b | d1 | e8 | 4f | 29 | c0 | b0 | e1 | e5 | c7 |
| | 1 | 74 | b4 | aa | 4b | 99 | 2b | 60 | 5f | 58 | 3f | fd | cc | ff | 40 | ee | b2 |
| | 2 | 3a | 6e | 5a | f1 | 55 | 4d | a8 | c9 | c1 | 0a | 98 | 15 | 30 | 44 | a2 | c2 |
| | 3 | 2c | 45 | 92 | 6c | f3 | 39 | 66 | 42 | f2 | 35 | 20 | 6f | 77 | bb | 59 | 19 |
| | 4 | 1d | fe | 37 | 67 | 2d | 31 | f5 | 69 | a7 | 64 | ab | 13 | 54 | 25 | e9 | 09 |
| | 5 | ed | 5c | 05 | ca | 4c | 24 | 87 | bf | 18 | 3e | 22 | f0 | 51 | ec | 61 | 17 |
| | 6 | 16 | 5e | af | d3 | 49 | a6 | 36 | 43 | f4 | 47 | 91 | df | 33 | 93 | 21 | 3b |
| | 7 | 79 | b7 | 97 | 85 | 10 | b5 | ba | 3c | b6 | 70 | d0 | 06 | a1 | fa | 81 | 82 |
| | 8 | 83 | 7e | 7f | 80 | 96 | 73 | be | 56 | 9b | 9e | 95 | d9 | f7 | 02 | b9 | a4 |
| | 9 | de | 6a | 32 | 6d | d8 | 8a | 84 | 72 | 2a | 14 | 9f | 88 | f9 | dc | 89 | 9a |
| | a | fb | 7c | 2e | c3 | 8f | b8 | 65 | 48 | 26 | c8 | 12 | 4a | ce | e7 | d2 | 62 |
| | b | 0c | e0 | 1f | ef | 11 | 75 | 78 | 71 | a5 | 8e | 76 | 3d | bd | bc | 86 | 57 |
| | c | 0b | 28 | 2f | a3 | da | d4 | e4 | 0f | a9 | 27 | 53 | 04 | 1b | fc | ac | e6 |
| | d | 7a | 97 | ae | 63 | c5 | db | e2 | ea | 94 | 8b | c4 | d5 | 9d | f8 | 90 | 6b |
| | e | b1 | 0d | d6 | eb | c6 | 0e | cf | ad | 08 | 4e | d7 | e3 | 5d | 50 | 1e | b3 |
| | f | 5b | 23 | 38 | 34 | 68 | 46 | 03 | 8c | dd | 9c | 7d | a0 | cd | 1a | 41 | 1c |

*Tabelul 2.3.12. Tabelul inverselor multiplicative în GF($2^8$) a octeților $(xy)_{16}$*

***Exemplul 2.3.6.*** Vom calcula inversul multiplicativ al lui $x^7+x^6+x$ în $GF\left(2^8\right)$. Reprezentarea binară a polinomului $x^7+x^6+x$ este $(11000010)_2$, iar valoarea hexazecimală corespunzătoare este $(c2)_{16}$. Inversul octetului $(c2)_{16}$ se află din Tabelul 2.3.12: acesta se găsește la intersecția liniei indexate cu $c$ și a coloanei indexate cu 2. Astfel, se obține inversul multiplicativ $(2f)_{16}$, care în reprezentare binară este $(00101111)_2$, iar în reprezentare polinomială - $x^5+x^3+x^2+x+1$. Într-adevăr, avem $\mathrm{mod}\left(\left(x^7+x^6+x\right)\left(x^5+x^3+x^2+x+1\right), m(x)\right)=1$. □

# SISTEMUL DE CRIPTARE AES

Din cele menționate la ultimele trei secțiuni rezultă că mulțimea $GF\left(2^8\right)$ din 256 de octeți, peste care este definită operația de adunare (XOR-ul biților octeților) și operația de înmulțire (se înmulțesc reprezentările polinomiale ale octeților modulo un polinom ireductibil) a elementelor, definește o structură de corp finit. Într-adevăr, mulțimea $GF\left(2^8\right)$ formează un grup aditiv comutativ în raport cu operația de adunare și un grup multiplicativ comutativ în raport cu operația de înmulțire, iar pentru orice elemente $a,b,c \in GF\left(2^8\right)$ se satisface legea distributivă a înmulțirii față de adunare $a(x)\cdot\left(b(x)+c(x)\right)=a(x)\cdot b(x)+a(x)\cdot c(x)$.

*2.3.5.2.1.4 Polinoame cu coeficienți în GF($2^8$)*

Vom considera polinoame de grad mai mic sau egal cu 3, $a(x)=a_3x^3+a_2x^2+a_1x+a_0$, ai căror coeficienţi $a_i$, $i=\overline{0,3}$, sunt elemente ale corpului octeților $GF\left(2^8\right)$. Polinoamele $a(x)$ pot fi reprezentate ca șiruri pe 4 octeți de forma $[a_0,a_1,a_2,a_3]$. Vom defini operațiile de adunare și de înmulțire a astfel de polinoame.

# SISTEMUL DE CRIPTARE AES

Să considerăm polinoamele

$$a(x)=a_3x^3+a_2x^2+a_1x+a_0,\ b(x)=b_3x^3+b_2x^2+b_1x+b_0,\ a_i,b_i\in GF\left(2^8\right),\ i=\overline{0,3}.$$

Operația de adunare a polinoamelor $a(x)$ și $b(x)$ definește un polinom $c(x)$ ai cărui coeficienți sunt obținuți prin adunarea în $GF\left(2^8\right)$ a coeficienților de pe lângă puterile asemenea ale lui $x$. Deoarece adunarea în $GF\left(2^8\right)$ este operația XOR pe biți, adunarea polinoamelor $a(x)$ și $b(x)$ corespunde operației XOR între octeții corespunzători ai fiecărui cuvânt:

$$a(x)+b(x)=(a_3\oplus b_3)x^3+(a_2\oplus b_2)x^2+(a_1\oplus b_1)x+(a_0\oplus b_0).$$

# SISTEMUL DE CRIPTARE AES

Operația de înmulțire a polinoamelor $a(x)$ și $b(x)$ este realizată în doi pași. La primul pas, se aduce la forma normală polinomul $c(x)=a(x)\cdot b(x)$:

$$c(x)=\sum_{i=0}^{6} c_i x^i ,$$

unde

$$c_0=a_0\cdot b_0,\ c_1=a_1\cdot b_0\oplus a_0\cdot b_1,\ c_2=a_2\cdot b_0\oplus a_1\cdot b_1\oplus a_0\cdot b_2,\ c_3=a_3\cdot b_0\oplus a_2\cdot b_1\oplus a_1\cdot b_2\oplus a_0\cdot b_3 ,$$

$$c_4=a_3\cdot b_1\oplus a_2\cdot b_2\oplus a_1\cdot b_3,\ c_5=a_3\cdot b_2\oplus a_2\cdot b_3,\ c_6=a_3\cdot b_3 .$$

Deoarece rezultatul $c(x)$ poate să admită o reprezentare pe mai mult de 4 octeți, la pasul doi se reduce $c(x)$ modulo un polinom de gradul 4, iar rezultatul este un polinom de grad mai mic sau egal cu 3. Polinomul de gradul 4 utilizat în algoritmul AES este $x^4+1$, astfel încât $\mathrm{mod}\left(x^i, x^4+1\right)=x^{\mathrm{mod}(i,4)}$

# SISTEMUL DE CRIPTARE AES

Rezultatul înmulțirii modulare a polinoamelor $a(x)$ și $b(x)$, notat prin $a(x) \otimes b(x)$, este dat de polinomul de gradul 3, $d(x)$, definit astfel:

$$d(x) = d_3 x^3 + d_2 x^2 + d_1 x + d_0,$$

unde

$$d_0 = (a_0 \cdot b_0) \oplus (a_3 \cdot b_1) \oplus (a_2 \cdot b_2) \oplus (a_1 \cdot b_3),\ d_1 = (a_1 \cdot b_0) \oplus (a_0 \cdot b_1) \oplus (a_3 \cdot b_2) \oplus (a_2 \cdot b_3),$$
$$d_2 = (a_2 \cdot b_0) \oplus (a_1 \cdot b_1) \oplus (a_0 \cdot b_2) \oplus (a_3 \cdot b_3),\ d_3 = (a_3 \cdot b_0) \oplus (a_2 \cdot b_1) \oplus (a_1 \cdot b_2) \oplus (a_0 \cdot b_3).$$

# SISTEMUL DE CRIPTARE AES

Când $a(x)$ este un polinom fixat, operația de înmulțire modulară poate fi scrisă sub formă matricială (matricea este de formă specială și anume o matrice circulantă) astfel:

$$\begin{pmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{pmatrix} = \begin{pmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}.$$

Efectul operației matriciale este rotația circulară a octeților cuvintelor de la intrare. Aceasta înseamnă că $[b_0, b_1, b_2, b_3]$ este transformat în $[b_1, b_2, b_3, b_0]$.

Deoarece $x^4+1$ nu este un polinom ireductibil peste $GF\left(2^8\right)$, înmulțirea cu un polinom fixat de gradul 3 poate să nu fie inversabilă. Cu toate acestea, algoritmul AES specifică un polinom de gradul 3, care are invers:

$$a(x)=\{03\}_{16}x^3+\{01\}_{16}x^2+\{01\}_{16}x+\{02\}_{16},\ a^{-1}(x)=\{0b\}_{16}x^3+\{0d\}_{16}x^2+\{09\}_{16}x+\{0e\}_{16}.$$

Un alt polinom utilizat în algoritmul AES are coeficienții $a_0=a_1=a_2=\{00\}_{16}$, $a_3=\{01\}_{16}$, adică este polinomul $x^3$.