UNIVERSITETI I PRISHTINËS “HASAN PRISHTINA”

FAKULTETI I SHKENCAVE MATEMATIKO – NATYRORE

Departamenti: Matematikë – Programi: Shkenca Kompjuterike



**Kodi i Cezarit**

Lënda: Siguri e të dhënave

Punuar nga: Erona Gashi, Benita Mehmeti

**Mars 2023**

Kodi i Cezarit

# Hyrje

Julius Cezari njihet për fitoret që i’a dhuroi Perandorisë Romake gjatë kohës së sundimit të tij. Gjithsesi, këto fitore nuk do të mund ti arrinte po të mos ishte edhe një strateg i shquar. Një ndër këto strategji që ai përdorte në mënyrë që të ishte gjithmonë një hap para armikut ishte edhe fshehja e mesazheve të drejtuara ndaj bashkëluftëtarëve të tij. Madje, metoda e tij e kriptimit të mesazheve, që njihet si Kodi i Cezarit (I emëruar sipas tij) ose Shifra e Cezarit, shënjon një ndër metodat më të vjetra të fshehjes së mesazheve si dhe fillin e një dege të tërë që tash njihet si kriptologji.

Kodi I Cezarit njihet ndryshe edhe si Kodi I Zhvendosjes për shkak se karakteristikë e tij është zhvendosja e shkronjave pasi për të dekriptuar mesazhin e kriptuar, duhet që shkronjat përbërëse të tij, sipas Cezarit, të zhvendosen për 3 vende.

Thyerja e Kodit të Cezarit tashmë është tejet e thjeshtë, mirëpo në kohën kur është përdorur, ky kod ishte efektiv për përcjelljen e mesazheve dhe informacioneve të vlefshme ushtarake.

# Historiku

Kodi i Cezarit është një ndër kodet më të hershme. I krijuar diku rreth vitit 100 para Krishtit, u përdor nga Julius Cezari për dërgimin e mesazheve sekrete te gjeneralët e tij në fushëbeteja. Kështu që, në rast se mesazhet e tij gjatë dërgimit mund të kapeshin nga armiqët e tij, ata nuk do të mund ti lexonin dhe kuptonin ato. Pikërisht kjo i dha atij një avantazh të madh strategjik [1].

Nuk është e ditur saktësisht se sa efektiv ka qenë Kodi I Cezarit në kohën kur është përdorur, mirëpo konsiderohet të ketë qenë racionalisht I sigurtë, duke pasur parasysh faktin se armiqët e Cezarit nuk kishin të paktën aftësi leximi, e lëre më aftësi të zbërthimit të kodeve.

Edhe pse Cezari ishte I pari që përdori një metodë të tillë për kriptimin e mesazheve, më vonë, edhe nipi i Julius Cezarit, perandori Augustus, përdori metodën e kriptimit me zhvendosje, mirëpo ai ndërroi numrin e zhvendosjes për 3 nga Cezari, në zhvendosje për 1 [2].

Në formën e përgjithshme ky lloj kriptimi bëhet duke bërë zhvendosjen e shkronjave për **k** vende, ku **k** paraqet një numër të plotë I cili mund të konsiderohet si celës. Ky kriptim poashtu është monoalfabetik, cka do të thotë se secili karakter zëvendësohet me karakter tjetër nga po I njëjti alfabet.

Kodi Vigenere përdorë parimin e Kodit të Cezarit, me një zhvendosje tjetër në secilin pozicion në tekst, ku vlera e zhvendosjes definohet duke përdorur një fjalë kyce përsëritëse. Nëse një fjalë kyce njëpërdorimëshe është zgjedhur në mënyrë të rastësishme, dhe është po aq e gjatë sa mesazhi, atëherë ky bëhet një kod I pa thyeshëm përderisa përdoruesit e tij ruajnë fshehtësinë e celësit [3].

Zhvendosja e Cezarit për 13 vende përdoret në algoritmin ROT13, një metodë kjo e thjeshtë e turbullimit të tekstit, e përdorur në disa forume Interneti për të errësuar (fshehur) tekstin, por nuk përdoret si një metodë e enkriptimit [4].

Enkriptimi mund të kryhet përmes aritmetikës modulare, duke I shëndrruar së pari shkronjat në numra sipas skemës: A=0, B=1, C=2,…, Z=25.

Formula për enkriptim:

En(x) = (x+n) mod 26

Formula për dekriptim:

Dn(x) = (x-n) mod 26

(Në rast se ndonjë herë Dn bëhet vlerë negative, atëherë kësaj vlere I shtojmë numrin 26).

# Avantazhet dhe disavantazhet

Benefitet e Kodit të Cezarit janë:

1. Është tejet I lehtë për tu implementuar;
2. Kjo metodë është metoda më e thjeshtë kriptografike;
3. Në të gjithë procesin e kriptimit dhe dekriptimit të mesazhit përdoret vetëm një celës I shkurtë;
4. Nëse një sistem nuk përdorë teknika komplekse të kodimit, atëherë Kodi I Cezarit është metoda më e përshtatshme;
5. Kërkon shumë pak resurse kompjutimi [5].

Mangësitë:

1. Mund të hakohet shumë lehtë. Pra, mesazhi I enkriptuar me këtë metodë mund të dekriptohet fare lehtë;
2. Ofron shumë pak siguri pasi është lehtë i dekriptueshëm;
3. I gjithë mesazhi mund të dekriptohet vetëm duke shikuar përsëritjen e shkronjave në të [6].

# Thyerja e Kodit të Cezarit

Pjesa më e vështirë e thyerjes së Kodit të Cezarit është gjetja e gjuhës së mesazhit që enkodohet. Në momentin që sulmuesi e gjen gjuhën në të cilën është shkruar mesazhi, ai konsideron dy mundësi. Njëra mundësi është përdorimi I teknikës së analizimit të shpeshtësisë së përdorimit të shkronjave të gjuha e caktuar, tjetra mundësi është përdorimi i brute force attack.

Të dhënat tregojnë se hera e parë e thyerjes së Kodit të Cezarit ka qenë në shekullit e 9-të pas Krishtit, përmes metodës së analizimit të shpeshtësisë së përdorimit të shkronjave, nga Al-Kindi [7].

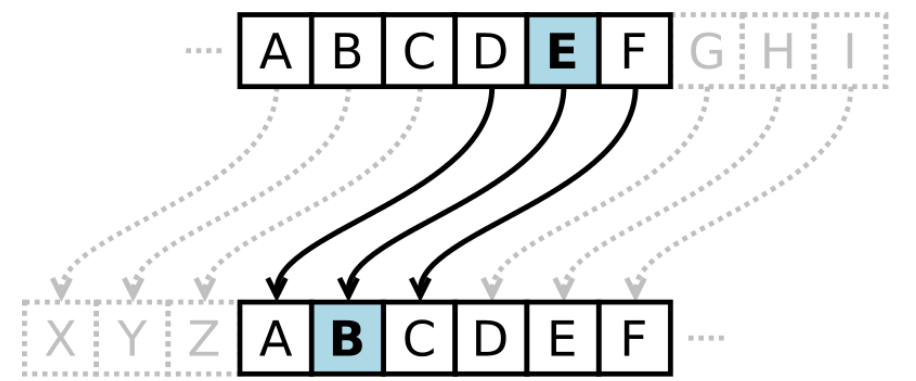
Brute force attack mund të bëhet duke konsideruar secilën zhvendosje të mundshme. Mesazhi përfundimtar do të ishte padyshim ai mesazh I cili bën sens në gjuhën e caktuar. Një tjetër mënyrë e përdorimit të brute force attack është shkrimi I alfabetit poshtë secilës shkronjë të mesazhit të enkriptuar, duke filluar nga ajo shkronjë. Kjo teknikë nganjëherë njihet edhe si “completing the plain component” [8].

Tjetra mënyrë e thyerjes së kodit është analizimi I shpeshtësisë së shkronjave në tekstin e koduar, kështu duke ditur shpërndarjen e mundshme të atyre shkronjave në gjuhën origjinale të tekstit të pa koduar, shumë lehtë mund të gjejmë numrin e zhvendosjeve, duke vërejtur keqpozicionimin e elementeve të caktuara në graf. Kjo metodë njihet si analiza e shpeshtësisë [9].

Distanca e unicitetit për Kodin e Cezarit është afërsisht 2, që nënkupton se të paktën dy karaktere të tekstit të koduar nevojiten për gjetjen e celësit.

Me Kodin e Cezarit nuk funksionon enkriptimi I shumëfishtë për rritjen e sigurisë së mesazhit. Kjo për shkak se zhvendosja për A dhe zhvendosja për B, të kryera një pas një, do të jetë ekuivalente me zhvendosjen A+B për një herë të vetme.

# Shembull



* **Përdorni Kodin e Cezarit për të kriptuar dhe dekriptuar mesazhin “HELLO”, nëse vlera e zhvendosjes është 15.**

## Enkriptimi

|  |  |  |
| --- | --- | --- |
| Shkronja: H → 07 | En: (07 + 15) mod 26 | Shkronja e kriptuar: 22 → W |
| Shkronja: E → 04 | En: (04 + 15) mod 26 | Shkronja e kriptuar: 19 → T |
| Shkronja: L → 11 | En: (11 + 15) mod 26 | Shkronja e kriptuar: 00 → A |
| Shkronja: L → 11 | En: (11 + 15) mod 26 | Shkronja e kriptuar: 00 → A |
| Shkronja: O → 14 | En: (14 + 15) mod 26 | Shkronja e kriptuar: 03 → D |

Mesazhi I kriptuar I tekstit “HELLO” është: **WTAAD**

## Dekriptimi

|  |  |  |
| --- | --- | --- |
| Shkronja e koduar: W → 22 | Dn: (22 - 15) mod 26 | Pas dekriptimit: 07 → H |
| Shkronja e koduar: T → 19 | Dn: (19 - 15) mod 26 | Pas dekriptimit: 04 → E |
| Shkronja e koduar: A → 00 | Dn: (00 - 15) mod 26 | Pas dekriptimit: 11 → L |
| Shkronja e koduar: A → 00 | Dn: (00 - 15) mod 26 | Pas dekriptimit: 11 → L |
| Shkronja e koduar: D → 03 | Dn: (03 - 15) mod 26 | Pas dekriptimit: 14 → O |

Dn = (00 - 15) mod 26 = -15 (Këtu vlera e Dn është negative, andaj I shtojmë numrin 26)

-15 + 26 = 11

# Referenca

[1]<https://ghostvolt.com/articles/cryptography_history.html#:~:text=Caesar%20Box,opponent%20could%20not%20read%20them>.

[2]<https://ghostvolt.com/articles/cryptography_history.html#:~:text=Caesar%20Box,opponent%20could%20not%20read%20them>.

[3] <https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/c/Caesar_cipher.htm>

[4]<https://ghostvolt.com/articles/cryptography_history.html#:~:text=Caesar%20Box,opponent%20could%20not%20read%20them>.

[5] <https://www.javatpoint.com/caesar-cipher-technique>

[6] <https://www.javatpoint.com/caesar-cipher-technique>

[7] <https://interestingengineering.com/innovation/11-cryptographic-methods-that-marked-history-from-the-caesar-cipher-to-enigma-code-and-beyond>

[8] <https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/c/Caesar_cipher.htm>

[9] <https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/c/Caesar_cipher.htm>