**UNIVERSITETI I PRISHTINËS “HASAN PRISHTINA”**

**FAKULTETI I SHKENCAVE MATEMATIKO-NATYRORE**

**DEPARTAMENTI I MATEMATIKËS**

**PROGRAMI: SHKENCA KOMPJUTERIKE**

**A picture containing logo

Description automatically generated**

Lënda: Siguria e të dhënave

Substitution Cipher

Punuar nga:

Nora Bytyqi

Redona Selmanaj

Mars 2023

**Përshkrimi**

Algoritmi Substitution Cipher është një teknikë kriptografike që përfshin zëvendësimin e çdo shkronje në plaintext me një shkronjë tjetër sipas një rregulle të caktuar. Rregulli i caktuar quhet "çelësi" dhe përdoret për të përcaktuar zëvendësimin e çdo shkronje.

Në një Substitution Cipher të thjeshtë, çelësi është një hartë e shkronjave të alfabetit në një set të tjera shkronjash. Për shembull, shkronja "A" mund të zëvendësohet me shkronjën "D", "B" mund të zëvendësohet me "E", dhe kështu me radhë. Çelësi zakonisht paraqitet si një tabelë, e quajtur tabela zëvendësuese, që tregon zëvendësimin për çdo shkronjë.

Për të enkriptuar një mesazh duke përdorur një këtë metodë, çdo shkronjë në plaintext zëvendësohet me shkronjën përkatëse në tabelën zëvendësuese. Për shembull, nëse tabela zëvendësuese harton shkronjën "A" me "D", "B" me "E", dhe "C" me "F", atëherë plaintext "HELLO" do të kriptohet si "KHOOR".

Siguria e kësaj teknike varet nga forca e çelësit. Nëse një sulmues mund të dyshojë ose të zbulojë çelësin, atëherë ata mund të dekriptojnë lehtësisht mesazhin. Prandaj, shifrat e zëvendësimit më komplekse përdorin teknika më të sofistikuara, si tabela të shumëfishta zëvendësuese ose çelësa me gjatësi të ndryshueshme, për të bërë më të vështirë që të thyhet shifrimi.

**Historiku**

Shifrimi zëvendësues është një nga format më të vjetra dhe më të thjeshta të teknikave të kodifikimit, me një histori që daton më shumë se 2,000 vite mbrapa. Besohet se shembujt më të hershëm të shifrave të zëvendësimit u përdorën nga grekët dhe romakët e lashtë për të mbrojtur komunikimet e tyre ushtarake dhe diplomatike.

Në fillimin e kriptografisë, shifrat e zëvendësimit shpesh krijohej duke përdorur teknika thjeshtë shkëmbimi të shkronjave, siç është shifra Caesar, që përfshinte shkëmbimin e secilës shkronje të alfabetit me një numër të caktuar pozicionesh. Megjithatë, me avancimin e teknikave të kriptanalizës, këto shifra të thjeshta nuk ishin më të mjaftueshme për të siguruar komunikim të sigurt.

Gjatë Mesjetës, u zhvillua një formë më të avancuar e shifrave të zëvendësimit, e njohur si "shifra Polialfabetike". Kjo shifër përdorte tabela të shumëfishta zëvendësuese, të cilat përdoren për të kodifikuar një shkronjë të vetme në plaintext. Çelësi i shifrës ishte një sekuenca shkronjash që përcaktonin cilën tabelë zëvendësuese do të përdorej për secilën shkronjë në plaintext.

Një nga shifrat e zëvendësimit më të famshme në histori është "Shifra Vigenere", e cila u zhvillua në shekullin e 16 nga kriptografi francez Blaise de Vigenere. Kjo shifër përdorte një seri shkronjash kyçe për të krijuar një model përsëritës të tabelave të zëvendësimit, duke e bërë shumë më të vështirë për t'u thyer në krahasim me shifrat e mëhershme të zëvendësimit.

Shifrat e zëvendësimit vazhduan të përdoren në të gjithë historinë, duke përfshirë edhe gjatë Luftës së Parë dhe së Dytë Botërore, kur ato u përdorën për të mbrojtur komunikimet ushtarake. Megjithatë, si fuqia e kompjuterit u rrit dhe u zhvilluan teknika të kriptimit më të sofistikuara, shifra e zëvendësimit u bë më pak e përdorur si një mjet për të siguruar komunikim të sigurt. Sot, ajo përdoret kryesisht si mjete mësimore për të prezantuar konceptet bazike të kriptografisë.

**Raste të përdorimit**

Algoritmi i Substitution Cipher mund të përdoret në një sërë raste përdorimi, duke përfshirë:

1. Komunikim konfidencial: Substitute cypher mund të përdoret për të mbrojtur konfidencialitetin e informacionit të ndjeshëm, siç janë komunikimet ushtarake ose diplomatike, sekretet biznesore ose mesazhet personale.
2. Edukim: Substitute cypher shpesh përdoret si mjet mësimore për t'u prezantuar konceptet bazë të kriptografisë dhe kodifikimit. Ata mund të ndihmojnë studentët të kuptojnë se si funksionon kodifikimi dhe si të krijojnë dhe thyjnë metodat bazë.
3. Lojëra dhe puzzles: Substitute cypher mund të përdoret në lojra ose gjuhëzime, siç janë dhomave të largimit(escape room), për të sfiduar pjesëmarrësit të dekodojnë një mesazh ose gjejnë një thesar të fshehur.
4. Steganografia: Substitute cypher mund të përdoret në lidhje me steganografinë, praktikën e fshehjes së një mesazhi brenda një mesazhi tjetër, për të bërë që të jetë edhe më e vështirë zbulimi ose dekodimi i tij.
5. Ruajtja historike ose kulturore: Substitute cypher është përdorur në të gjithë historinë nga kultura dhe qytetërimet të ndryshme, dhe studimi i tyre mund të ndihmojë në ruajtjen dhe kuptimin e rëndësisë kulturore dhe historike të kriptografisë.

**Shembull**

Teksti i mëposhtëm është enkriptuar me metodën e zëvendësimit, ku është përdorë njëri nga 26! alfabetet. Dekriptoni tekstin duke përdorë metodën e frekuencave relative, duke u bazuar në tabelën nga ushtrimet. Teksti është enkriptuar ashtu që shenjat e pikësimit, numrat si dhe shkronja Ë kanë mbetur të njëjta, ndërsa shkronjat tjera janë zëvendësuar.

Teksti:

*COSKGËBKR RCDNËOJBË DLV VR GRCLB DNË GIAKFKVË FË SRBFË GËBVLDUBJNF EIFËC COSKGFRBJ DË ERAAVRD. RNI SË CGKVRF CK GIAKFKVË SË DMR QKFK 1920, ËCOFË PRVFK K GBIQLRB FRCOHË SË SJQJBKFË COSKGFRBJ, SË DMR ROHJF ZIML J UJBK FJ CRAK EJBKCOR, DLV VRDË ALRNFLB PRBJ GËB FË VIDCIAKULRB DNË GIAKFKVË CFBRFJMNKVJ DË PLDVCKID FË EIFËC COSKGFRBJ DË ERAAVRD. GËBVLDUBRZK, VËFI SJQJBK DLV J VRDË GRCLB PRBJ DË VIDCKUJBRFË OKCFIBKDË J RDJVCKHJQJ FË DNËGRCDNËCOHJ SË K NRDË EËBË FJBBKFIBJQJ COSKGFRBJ DMR PSKDNËF, UOJ, GIAKFKVKCOF, VRDË ALRNFLB DË PRQIB FË PSKDNËQJ RDJVCLJC GËB FË HRBBË ICJ GËB FË HERNFLB GLCOFJFKD J FYBJ GJBCIDRA DË COSKGËBK .........*

**Zgjidhje**

Në një listë, do të renditen të gjitha shkronjat e tekstit prej asaj që është përsëritur më së shumti deri te ajo që është përsëritur më së paku. Shkronja e parë që është përsëritur më së shumti në tekst do të zëvendësohet me shkronjën e parë me frekuence më të lartë, pra “E”. Ngjashëm për shkronjat e tjera. Në fund dekriptohet teksti dhe përmirsojmë gabimet që kanë ndodhur në tekstin e dekriptuar.

**Klasa *RelativeFrequencies***

Klasa RelativeFrequencies është klasa në të cilën meret teksti, dhe krijohet tabela e sortuar se sa hërë një shkronjë është përsëritur në tekst. Pastaj secila shkronjë do të zëvendësohet me shkronjat nga frekuencat relative.

Përdorim strukturën e të dhënave *Map<String, Integer> ,* në të cilën do të mbushën te dhë\nat se sa herë një shkronjë përsëritet. Iterojmë në secilën shkronjë të tëkstit dhe inkrementojmë vlerën për atë shkronjë se sa herë është përsëritur. Pastaj sortojmë listën në bazë të shkronjës së shfaqur më së shumti deri te ajo më së paku.

    for (int i = 0; i < text.length(); i++) {

            try {

                z = text.charAt(i);

                map.put(String.valueOf(z), map.get(String.valueOf(z)) + 1);

            }

            catch (java.lang.NullPointerException e) {

            }

Map-i jonë përmban vetëm shkronja, por jo simbole e as numra. Kshtuqë kur iterojmë në tekst, do të na shfaqet ndonjë simbol apo numër. Nëse tëntojmë ta vendosim këtë të simbol në map, do të na shfaqet një error, prandaj ne shfrytëzojmë sintaksën try catch për të injoruar të gjitha simbolet tjera përspos numrave. Pas ekzekutimit të këtij kodi do të marim:

{1933=J, 1897=Ë, 1855=K, 1841=F, 1553=R, 1440=B, 1384=D, 1284=C, 946=O, 941=V, 911=I, 758=G, 694=U, 580=A, 564=N, 537=H, 513=L, 391=S, 261=Q, 219=E, 196=M, 165=P, 98=Y, 93=T, 79=Z, 8=X, 0=Ë}.

Dmth shkronja J duhet të zëvendësohet me shkronjen e parë me frekuence më të lartë relative të alfabetit shqip, pra me E, e kështu me radhë, dhe fitojmë:

|  |  |
| --- | --- |
| J | E |
| Ë | Ë |
| K | T |
| F | I |
| R | A |
| B | R |
| D | M |
| C | S |
| O | H |
| V | U |
| I | K |
| G | O |
| U | M |
| A | D |

|  |  |
| --- | --- |
| N | J |
| H | P |
| L | L |
| S | G |
| Q | V |
| E | B |
| M | Q |
| P | F |
| Y | Z |
| T | Y |
| Z | C |
| X | Ç |
| Ë | X |

Prap iterojmë në secilën shkronjë të tekstit dhe zëvendësojmë secilën shkronjë me zëvendësimin përkatës, psh J zëvendësohet me E, K zëvendësohet me T e kështu me radhë përmes metodes textDecrypt.

  public static String textDecrypt(String text, Map<String, String> map3) {

        String text2 = "";

        char z;

        for (int i = 0; i < text.length(); i++) {

            z = text.charAt(i);

            try {

                text2 += map3.get(String.valueOf(z)).charAt(0);

            }

            catch (java.lang.NullPointerException e) {

                text2 += String.valueOf(z);

            }

        }

        return text2;

    }

Metoda text decrypt zëvendëson secilën shkronjë të tekstit bazuar nga një rregulle(Map) . Pas ekzekutimit fitohet:

*SHGTOËRTA ASNJËHERË NLU UA OASLR NJË OKDTITUË IË GARIË OËRULNMREJI BKIËSSHGTOIARE NË BADDUAN. AJK GË SOTUAI ST OKDTITUË GË NQA VTIT 1920, ËSHIË FAUIT TORKVLAR IASHPË GË GEVERTIË SHGTOIARE, GË NQA AHPEI CKQL E MERT IE SADT BERTSHA, NLU UANË DLAJILR FARE OËR IË UKNSKDTMLAR NJË OKDTITUË SIRAIEQJTUE NË FLNUSTKN IË BKIËS SHGTOIARE NË BADDUAN. OËRULNMRACT, UËIK GEVERT NLU E UANË OASLR FARE NË UKNSTMERAIË.*

Prej nga kuptojmë gabimet që duhet të përmirësuar.

|  |  |
| --- | --- |
| G | Q |
| T | I |
| O | P |
| L | U |
| U | K |
| D | L |
| I | T |
| P | M |
| K | O |
| M | D |
| C | Z |
| Y | C |
| Q | G |
| Z | Y |

Pas zëvendësimit të këtyre shkronjave do të marim tekstin:

SHQIPËRIA ASNJËHERË NUK KA PASUR NJË POLITIKË TË QARTË PËRKUNDREJT BOTËS SHQIPTARE NË BALLKAN. AJO QË SPIKAT SI POLITIKË QË NGA VITI 1920, ËSHTË FAKTI I PROVUAR TASHMË QË QEVERITË SHQIPTARE, QË NGA AHMET ZOGU E DERI TE SALI BERISHA, NUK KANË LUAJTUR FARE PËR TË KONSOLIDUAR NJË POLITIKË STRATEGJIKE NË FUNKSION TË BOTËS SHQIPTARE NË BALLKAN. PËRKUNDRAZI, KËTO QEVERI NUK E KANË PASUR FARE NË KONSIDERATË HISTORINË E ANEKSIMEVE TË NJËPASNJËSHME QË I JANË BËRË TERRITOREVE SHQIPTARE NGA FQINJËT, DHE, POLITIKISHT, KANË LUAJTUR NË FAVOR TË FQINJËVE ANEKSUES PËR TË MARRË OSE PËR TË MBAJTUR PUSHTETIN E TYRE PERSONAL NË SHQIPËRI...

**class RelativeFrequences**

|  |  |
| --- | --- |
| Konstruktori |  |
| *RelativeFrequences*(String text) | konstrukton një objekt të ri bazuar tekstin e enkriptuar |
| Atributet |  |
| String[] alphabet | alfabeti në gjuhën shqipe |
| String[] frequencies | frekuencat e gjuhës shqipe |
| Map<String, Integer> map | mban të dhëna për numrin e paraqitjes së shkronjave në tekst |
| Map<String, Integer> map3 | shkrojat përkatëse me cilat shkronja duhen të zëvendësuar bazuar në frekuencat relative. |
| Metodat |  |
| public String textDecrypt(String text, Map<String, String> map3) | dekripton një tekst bazuar me metodën e zëvendësimit të secilës shkronjë sipas rregulles map |
| private String[] fill(String word) | kthen një array të tipit String me karakteret e fjalës word. |