1 Caesar

Algoritmul lui Caesar este un algoritm simetric, care se foloseste de un alfabet cu caracterele aferente pe pozitii diferite.

Acest algoritm are doua variante, algoritmul care se foloseste de o cheie si un numar care reprezinta valoare de ,,shift"-are a literelor in alfabet.

Algoritmul care a fost implementat in aceasta aplicatie este cel cu cheie si valoare dar, oferind optiunea de a omite cheia.

Pasi urmatori reprezinta ce se intampla in spatele interfetei:

1. Se creaza un obiect de tipul clasei ,,Caesar" folosind constuctorul cel mai potrivit.
2. Se verifica validitatea informatiior introduse.
3. In cazul incriptari textului se vor intampla urmatoarele:
   (a) In cazunl in care nu a fost precizata o cheie, se va genera una de lungime 10 avand caractere aleatoare intre 'a' si 'z'. Daca sa precizat o cheie aceasta va fi folosita in schimb.

   Daca nu se doreste folosirea unei chei este necesar sa existe un caracter care nu este o litera in casuta cheii.

   (b) Se va genera un alfabet in memorie care respecta indicatiile cifrului. Daca exista o cheie, caracterele unice ale acesteia se vor afla la inceputul alfabetului urmate de restul caracterelor din alfabetul englez, in caz contrar se va genera un alfabet normal.

(c) Dupa acesti pasi de pregatire se va parcurge fiecare caracter introdus si se va alege un caracter din alfabetul generat care se afla pe aceasi pozitie ca si in alfabetul normal plus valoarea de shiftare.

4. In cazul decriptarii textului se vor intampla urmatoarele:

   (a) Se verifica existenta unei chei, daca aceasta nu a fost precizata se va returna un mesaj de informare. Daca se doreste o decriptare fara cheie este necesar sa existe un caracter care nu este o litera in casuta cheii.

   (b) In continuare va crea un alfabet cu cheia de la punctul anterior.

   (c) Fiecare carafter din mesaj va fi parcurs si se va crea un text, litera decriptata va fi pozitia din alfabetul generat minus valoare de shiftare, aceasta pozitie va reprezenta pozitia din alfabetul normal a literei.

Observatii:

- Programul poate accepta si caractere care nu sunt lidere doar ca acestea vor fi ignorate.
- Programul va returna un text normalizat cu toate caracterele mici.
- Lungimea maxima a cheii este de 25 de caractere.
- Cheia generata folositnd optiunea de ,,New key" va avea lungimea de 10 caractere
- Textul din campul ,,Normal Text" in urma apasarii butonului ,,Encrypt" va fi criptat si afisat in campul ,,Encrypted Text". Acelasi lucru se intampla in sens invers in cazul butonului ,,Decrypt".

2 Playfair

Algoritmul Playfair este un algoritm simetic care se foloseste de tabela Polybul pentru a incripta mesajele. Exista doua variante a acestui algoritm, cel cu cheie si cel fara cheie. In aplicatia curenta s-a implementat cel cu cheie dar cu optiunea de a putea fi ignorata.

Acest tabel este reprezentat de literele alfabetului englez aranjate in forma unei matrici cu cinci linii si cinci coloane, caracterul 'j' va fi transformat in 'i' la incriptare.

Pasi algoritmului sunt uramtorii:

1. Se verifica daca datele introduse sunt corecte.
2. Se va crea un obiect de tipul clasei ,,Playfair" care va primi ca si parametii nimic sau cheia data.

3. Se va crea matricea. In cazul existentei unei chei se va schimba alfabetul astfel incat literele unice ale cheii sa se afle la inceputul acestuia urmate de restul literelor.

4. In cazul incriptari se vor intampla urmatoarele:

   (a) Se verifica daca exista un numar par de litere in mesajul introdus.

   (b) In cazul in care nu exista un numar par se va adauga litera 'z' la sfarsitul mesajului.

   (c) Se parcurge fiecare caracter al mesajului luand un grup de doua caractere si se verifica in ce situatie se regasesc.

      - In cazul in care caracterele se afla pe aceasi coloana se va alege litera pe pe randul urmator al fiecarui caracter.
      - In cazul in care se afla pe acelasi rand se vor alege caracterele de pe coloana urmatoare fiecarui caracter.
      - in cazul in care se afla pe randuri si coloane diferite se vor alege literele de pe acelasi rand dar coloana in care se afla cealalta litera.

5. In cazul decriptari se vor intampla uramtoarele:

   (a) Se verifica daca exista un numar par de litere in mesajul introdus. In caz contrar se va afisa un mesaj de informare care spune ca textul introdus nu este adecvat.

   (b) Se parcurge fiecare caracter al mesajului luand un grup de doua caractere si se verifica in ce situatie se regasesc.

      - In cazul in care caracterele se afla pe aceasi coloana se va alege litera pe pe randul anterior al fiecarui caracter.
      - In cazul in care se afla pe acelasi rand se vor alege caracterele de pe coloana precedenta fiecarui caracter.
      - in cazul in care se afla pe randuri si coloane diferite se vor alege literele de pe acelasi rand dar coloana in care se afla cealalta litera.

Observatii:

- Programul poate accepta si caractere care nu sunt lidere doar ca acestea vor fi ignorate.
- Programul va returna un text normalizat cu toate caracterele mici.
- Lungimea maxima a cheii este de 25 de caractere.
- Cheia generata folositnd optiunea de ,,New key" va avea lungimea de 10 caractere
- Textul din campul ,,Normal Text" in urma apasarii butonului ,,Encrypt" va fi criptat si afisat in campul ,,Encrypted Text". Acelasi lucru se intampla in sens invers in cazul butonului ,,Decrypt".

3 RSA (Rivest–Shamir–Adleman)

RSA este un algoritm de criptare care se foloseste de doua chei, una publica si una privata.

Pentru incriptarea mesajelor este folosita cheia publica, iar pentru decriptare este folosita cea privata.

Cheile sunt generate pe baza a doua numere prime de regula foarte mari(mai mare de 1024 biti). Prima parte care alcatuieste si cheia publica si cheia privata denumita ,,N" este contruita pe baza formulei (p-1)*(q-1) unde 'p' si 'q' sunt cele doua numere prime. A doua parte a cheii publice este un numar intre 1 si 'N' care este si coprim cu 'N', aceasta parte numinduse ,,E". A doua parte din cheia privata numit ,,D" este un numar care respecta formula (D*E=1 mod N), ,,D" fiind de regula un numar foarte mare.

Aplicatia ofera posibilitatea de a genera cheile pe baza factorilor 'p' si 'q', de a utiliza chei deja existente sau de a genera chei noi cu 'p' si 'q' decisi aleator.

Pasi algoritmului sunt urmatorii:

1. Se verifica daca exista chei introduse(toate valorile trebuiesc sa fie mai mari ca si 0) sau daca sunt introdusi factorii.
2. In cazul existentei factorilor acestia se vor folosi pentru generarea cheilor.
3. Se va crea obiectul de tipul clasei ,,RSA" adecvat inputului.
4. In cazul in care nu au fost precizati factori sau cheile, se vor genera chei aleatoare cu o factori intre 1.000 si 200.000
5. In cazul incriptarii se va proceda astfel:
   (a) Se va parcurge fiecare caracter al mesajului si se va aplica formula (m*,,E") mod ,,N" unde 'm' reprezinta valoare caracterului in tabelul ASCII
   (b) In urma pasului anterior se va genera un mesaj format din numere separate prin spatiu.
6. In cazul decriptari se va proceda astfel:
   (a) Se verifica validitatea textului.
   (b) Se verifica existenta cheilor, in caz contrar se va emite un mesaj de informate in cere este precizata necesitatea lor.
   (c) Se va parcurge fiecare valoare din mesaj si se va aplica formula (c*,,E") mod ,,N" unde 'c' reprezinta valoare respectiva.
   (d) In urma pasului anterior se va genera mesajul original.

Observatii:

- Programul accepta toate caracterele care se regasesc in tabelul ASCII.
- 'P' si 'Q' trebuiesc obligatoriu sa aibe produsul mai mare ca 127 din cauza motivului precedent.
- In cazul in care se utilizeaza factorii 'P' si 'Q' se vor genera chei noi chear daca deja exista chei introduse.
- In cazul in care nu se utilizeaza factorii, daca oricare valoare a cheilor este '0' se vor genera chei noi.
- In momentul in care se genereaza chei aleatoare aplicatia va bloca interfata pana ce se vor termina de generat cheile.
- Textul incriptat trebuie sa contina doar numere si spatii altfel va aparea un mesaj de informare.
- Valoare 'E' va fi de regula foarte mica dar spre deosebire 'D' va fi extrem de mare din motifve de optimizare.