7-amaliy ish

Mavzu: RC4 shifrlash algoritmi asosida ma’lumotlarni shifrlash va deshifrlash dasturini yaratish

Ishdan maqsad: RC4 shifrlash algoritmi haqida nazariy va amaliy bilim ko’nikmalarga ega bo’lish.

Nazariy qism

RC4 – uzluksiz shifrlash algoritmi bo‘lib, u SSL(Secure Sockets Layer) pratakoli va WEP (simsiz tarmoqlarda xavfsizlikni ta’minlashda) keng foydalaniladi. RC4 uzluksiz shifrlash algoritmi Ron Rivest tomonidan 1987 yilda yaratilgan va shuning uchun RC4(Rivest Cipher 4) deb nomlangan.

RC4 psevdotasodifiy bitlar ketma-ketligini hosil qiladi va hosil qilishda ikki qismdan iborat bo‘lgan maxfiy oraliq xolatidan foydalaniladi:

-barcha mumkin bo‘lgan 256 baytning joylashishdagi o‘rni(S ni topish);

-ikkita 8 – bitli indekslar (*i* va *j* larni topish).

Baytlarning kelish tartibi kalit uzunligi bilan amalga oshiriladi, odatda 40-256 bit oralig‘ida bo‘lib, kalit jadvali (key-scheduling) algoritmi orqali hosil qilinidi. Bu jarayon tugagandan so‘ng psevdotasodifiy sonlar generatori algoritmi yordamida bitlar ketma-ketligi hosil qilinadi.

Kalit jadvali algoritmi quyidagicha (1-algoritm):

for i from 0 to 255

S[i] := i

endfor

j := 0

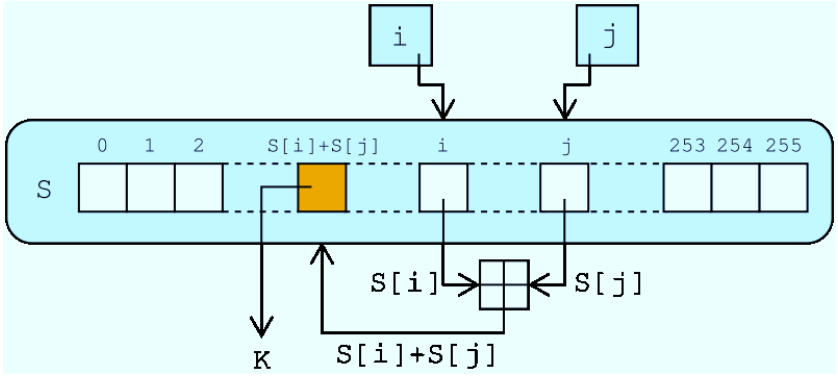
for i from 0 to 255

j := (j + S[i] + key[i mod keylength]) mod 256

swap values of S[i] and S[j]

endfor

Psevdotasodifiy sonlar generatori algoritmi orqali hosil bo‘lgan ketma-ketlik tanlangan S(i) va S(j) o‘zgaruvchilarni mod256 bo‘yicha qo‘shishdan hosil bo‘ladi (7.1- rasm).



7.1-rasm. RC4 generatori almashtirishi

Psevdotasodifiy sonlar generatori algoritmi quyidagicha (2-algoritm):

i := 0

j := 0

while GeneratingOutput:

i := (i + 1) mod 256

j := (j + S[i]) mod 256

swap values of S[i] and S[j]

k := S[(S[i] + S[j]) mod 256]

output k

endwhile

Algoritmda i o‘zgaruvchini qiymati ortishi bilan hosil bo‘lgan baytlar soni ham ortib boradi.

Bu yerda almashtirish funksiyasi swap quyidagi ko‘rinishga ega (3-algoritm):

byte temp = array[ind1];

array[ind1] = array[ind2];

array[ind2] = temp;

Ushbu generator kriptobardoshli sanalib, ushbu xususiyat kiruvchi kalit tasodifiylik darajasi bilan belgilanadi. Hozirda ushbu algoritmning bir nechta

variantlari mavjud bo‘lib(RC4A, VMPC, RC4+), ularda dastlabkilarida mavjud kamchiliklar bartaraf etilgan.

Yuqorida keltirilgan algoritm kalit generatori algoritmi sanalib, agar ushbu algoritm shifrlash algoritmiga o‘zgartirilsa faqat 2-algoritm quyidagicha o‘zgaradi (4-algoritm):

i := 0

j := 0

while GeneratingOutput:

i := (i + 1) mod 256

j := (j + S[i]) mod 256

swap values of S[i] and S[j]

C := plainText XOR S[(S[i] + S[j]) mod 256]

output C

endwhile

Bu yerda: plainText - shifrlanishi kerak bo‘lgan ochiq matn.C- shifrmatn.

Amaliy qism:

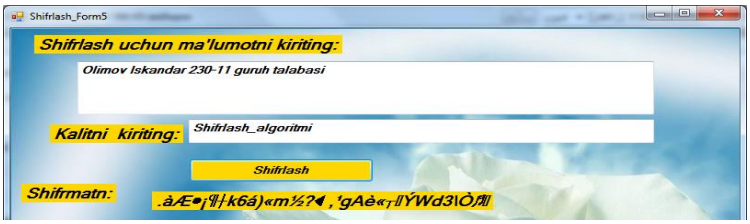
RC4 oqimli shifrlash algoritmining dasturiy ta’minotini ishlab chiqishda c# , Eclipse IDE for Java Developers - 2020-03 va jdk-14.0.1 obe’ktga mo‘ljallangan dasturlash tillaridan foydalanilgan bo’lib, dasturni ishga tushurganimizda quydagi oyna paydo bo’ladi.

7.2-rasm. Dasturni umumiy ko’rinishi

Dasturdan foydalanish uchun tugmani ishga tushurganda : dasturdan foydalanish haqida yo’riqnoma chiqadi.

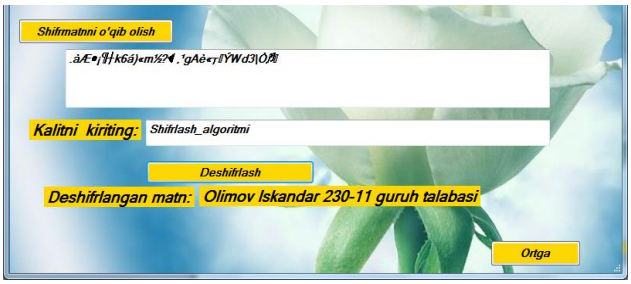
Shifrlash va deshifrlash tugmasini bosganingizda:

- ochiq ma’lumot kiritiladi
- kalit kiritiladi



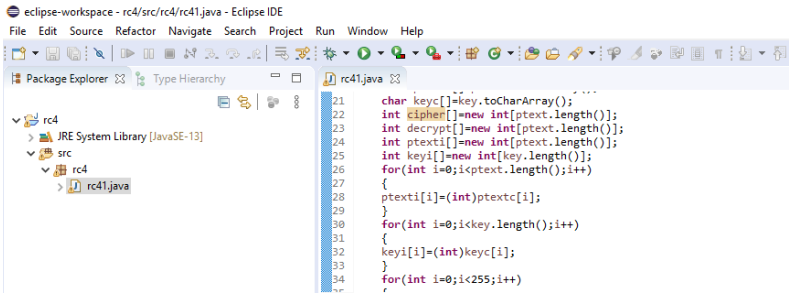
7.2.1-rasm. Shifrlash jarayoni

Deshifrlash uchun shifrmatnni o‘qib olish tugmasini bosganingizdan so‘ng kalitni kiritiladi va deshifrlash tugmasini bosamiz:

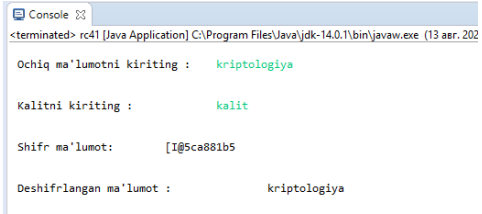


7.2.2-rasm. Deshifrlash jarayoni

RC4 shifrlash algoritmi Eclipse IDE for Java Developers - 2020-03 dasturlash tilida.



7.2.3-rasm. Dasturni umumiy ko’rinishi



7.2.3-rasm. Shifrlash va deshifrlash natijalari

Ishni bajarilish tartibi va qo’yilgan vazifa

Asosiy matn shifrlash usullarida shifrlansin va qadamma – qadam izohlansin. Shuningdek *Delpi, Java, C++* va *C#* dasturlash tizimlaridan birida dasturiy ta’minot yaratilsin**.**

Nazorat savollari

1. Oqimli simmetrik algoritmlar haqida umumiy tasnif
2. RC4 shifrini tavsiflang.
3. Oqimli shifrlash algoritmlar tarkibiga kiruvchi algoritmlar?