Министерство образования Республики Беларусь
Учреждение образования
“Брестский государственный технический университет”
Кафедра интеллектуально-информационных технологий

Лабораторная работа №3
“Атака на алгоритм шифрования RSA посредством метода бесключевого чтения”

Выполнил:
студент 4 курса
группы ИИ-22
Клебанович В. Н.
Проверила:
Хацкевич А. С.

Брест 2024

Цель работы: изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Ход работы:

- ознакомиться с теорией;
- по исходным данным определить значения r и s пр условии, что e1*r - e2*s = 1. Для этого необходимо использовать расширенный алгоритм Евклида;
- используя значения r и s, получить исходный текст;
- результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформить в виде отчета.

Код программы:

```
N =
25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357

e1 = 1011163
e2 = 1110521

C1 =
77754652948361380460014312242632688587614544232225399697892740593465521376368465285951984880057065511217090693365520203095739375941820666985951356240239221530219804642924532777938770906461185321168292692822624932430751736964659174722512846447501243114334851807478860765118766619992243759626576318048945905270848431464978407514962577461060085509160935241801157514873032579136325108799396735269694185643159141440788742008016661216756517349328299325883311290816460991200316300200428430571143284891710113688791628187620045869750036851496465226054496455553492525518706913666759248665070989987465152551112221380732480915230
C2 =
80073973348096677452203000391265340736982988270173795195688766780
```

```
747821690784519593639038488347148864300022732245237197967208291784675475153428789606927364675249476940968515888652062218549615954103803766817615290350469862654789232661043591282886759451257718695549999365578294233621566772607776976533936507285262087779730495465840453056008406246824422771917914589821798419980798495594506997754489980370730474209604492532865548204254300729469845384385839714643589750275166249372315044940828770149403795366250361919386556801545691360732071667085569617551061682104181457101985794668864580190086037341569043963263828848922

A = e1
B = e2
C = 169131
D = 185750

result = A * D - B * C
print("\nA * D - B * C =", result)

r = D
s = C

mod = N

result1 = pow(C1, r, mod)

print("\nC1^r =", result1)

result2 = pow(C2, -s, mod)

print("\nC2^(-s) =", result2)


m = result1 * result2

print("\nm^(e1 * r + e2 * s) =", m)

result3 = pow(m, result, mod)

print("\nm^-(e1 * r + e2 * s)modN =", result3, "\n")
```

Вывод программы:

```
A * D - B * C = -1

C1^r = 240884243073801055461017568597771138334778898738296423725367554605013768139609289714376077743522222752084660659397833177586
308610773388100645529592911770015999971739883946234526527322257557865437715473143173405826873874241196080645446995266734559553931 2
702361459401848018967166219940166962839805711411908346204608615830030403748221979315173569232562956869352346098428707065758069484 9
858524859526397680729327195256363144423118532506575628096915407741880345952391423509412265938351877078464021058167916651484462067 1
72704772003670557560349330250116287301153196512479695760945610788218479197055521228307270222989147963138

C2^(-s) = 224826698633279322280433416228797972218571429577555880145961867061999506532460268807136056502525036554000206778154733796
775916340454614834680999687896804896352730096988166397657509376414506808331637588058749533600949055405475182362992896759146879502 5
420945547733575466071578470688436464380247246035968224500940026840442334730944164397713755360772523631095626994435670184979533583 3
111902535629122068820750260188752306490805757935337361376755162547120426140521435615181280404570606292315036084831880598486304697 2
296993568199497484078487311535105265262689077779209293498481262464906117719277668564007914686353723201803 88

m^(e1 * r + e2 * s) = 541572091230590718100273672339371749052243083494003363408556302981385406334478321488860907226910926531013801
858420937890953813543683942655919268465119743723054112664890368960990761375735502123751001132445687902229565905435386972264809469 6
295177705139756222739087417543799970755207068362053946645973383102281778989782810264404626422479797488120343667694919516759863073 6
902166298529257384304158988833980699323669966445447243913046008953129589710687424969704248978794358997664883326882471288495480214 2
250619319739227313338609600941071296441734876103302037707924430525660684563838198549685508967824437528770728879342992629391938097 2
243135185608646270164627266869540316178239145938746879833080198983011069489767091749400349784315647695338581847550796346493831576 6
344817416144908390421531259926759854848408087245216518645362621439740406999660799266100002390490672884197779832143275879726606711 4
002454537307907511355822327927518854755594710911013665951872764900005794753073245073138538182137686161407622651956105053110794482 2
188047962024698436894720652077400640361090238343521956557953336629915888561362476230418625370808529128442696643232223560466780272 3
174696666396707408443860234072294914767641773033005914543212271304373083196293453754 4

m^-(e1 * r + e2 * s)modN = 267989235247753055496706261812300201403744155866912015336589661563708063175304058124939739611563377553 2
404890107934891832314235549036285113280517136606896417
```

Вывод: освоил на практике основные принципы создания систем анализа и синтеза речи.