МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
“БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ”
ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Отчёт
по дисциплине
Современные методы защиты компьютерных систем
по лабораторной работе №3
«Атака на алгоритм шифрования rsa»

Выполнил:
Студент группы ИИ-22
Борейша О.С.
Проверил:
Хацкевич А. С.

Брест 2024

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

Задачи:

1. Ознакомиться с теорией.
2. Получить вариант задания у преподавателя.
3. Программно реализовать алгоритм атаки.

Код программы:

```
def extended_gcd(e1, e2):
    x0, x1, y0, y1 = 1, 0, 0, 1
    while e2 != 0:
        q, e1, e2 = e1 // e2, e2, e1 % e2
        x0, x1 = x1, x0 - q * x1
        y0, y1 = y1, y0 - q * y1
    return e1, x0, y0


def find_coefficients(e1, e2):
    gcd, x, y = extended_gcd(e1, e2)
    if gcd == 1:
        r, s = -x, y
    elif gcd == -1:
        r, s = x, -y
    else:
        raise ValueError("Невозможно найти коэффициенты, так как НОД(e1, e2) !=
±1")
    return r, s


def mod_inverse(a, mod):
    gcd, x, _ = extended_gcd(a, mod)
    if gcd != 1:
        raise ValueError(f"Обратное значение для {a} по модулю {mod} не суще-
ствует")
    else:
        return x % mod


e1 = 1302293
e2 = 1300367
r, s = find_coefficients(e1, e2)

print(f"Коэффициенты: r = {r}, s = {s}")
print(f"Проверка: {r} * {e1} - {s} * {e2} = {r * e1 - s * e2}")

N =
11168908155396125547532407185205385017208097433775964348252922061124205562450889605893438208177204063073142960614153642736025426431890488245790444591999505073762871716810108379781397800567873193788261542187332784808057984070138848433410380038755129122300260693387026828115617834705460275265561276317424303897317733328825206401110932599440172712327838994078236814739804332838665774117619433110401757533427657380076667308948789610055979217942460819777703854388318398175416179806446968188588671615522115139621711103195510022865344245629204457377895174216750426938368933678497045069789946569550170810238300129206612786887
C1 =
66586582039290704038174083161924184389634137899089371089409988272180058638640255033861428779222819508672272895488891560357720829887632361677839270328140807076880115430600307156930995967538571121617260621666976507892531521898172319349661474531088918151057967833222529791819366268979556913005862935442020886123790718483586465993841208404018198304045275306157335708327900746119985396739202937012923796777178508275286295786689691770556564032201406644938811452584813826893297427513632309178215309
```

```
475037291151404360445296818033657577888336230183478041961636168893384990237028153029671811799379698235900386359585441324 27
C2 =
376413086329343120768282613409904977500621082073241071141381917019310616279958869005174743858852514439382305368236029625888827103175402446215902433890846381489662787779923537473208336182465991969947176792138755338127105004089711692824648289501114654284002987373837592736593561888848835852186651764785793872457701240081661967986232270284385327479027316706064410005648274228534512136714823450352089753437036101312063150577656643121093984522849873712936554871800335015158122072800251801157574372311743578196092785873904700063882322322194655114819564886343235983941678682859180949823036165412243093504460558595757195733

c1 = pow(C1, r, N)
c2 = pow(C2, -s, N)
print(f'c1**r = {c1}\nc2**(-s) = {c2}')

multiplication = (c1 * c2)
print(f'multiplication result = {multiplication}')

result = mod_inverse(multiplication, N)
print(f'result = {result}')

result_bytes = result.to_bytes((result.bit_length() + 7) // 8, byteorder='big')  # Преобразуйте в байты
decoded_message = result_bytes.decode('windows-1251')  # Используйте 'windows-1251' для кириллицы
print(f'Расшифрованное сообщение: {decoded_message}')
```

Результат работы:

```
Коэффициенты: r = 270741, s = 271142
Проверка: 270741 * 1302293 - 271142 * 1300367 = -1
c1**r = 3147537546068979521088581207878527895362018849236245516482550376374187380098103077585520084190879924943634153592341257109358706433230140845960187409082479400263649788392548329667236880004508895337680177299136312764851650283753864717428837514756979729489398243383512833745056805378794703024168535234671850411769843007928065842528124387999030071122408358216248376809397840408228384047544868685317170860623479760080318721582724011840719731242589218461303900473098143544772075069751256763991525485780523370602412926332081883320069986494875157859989300477927205329448906004596470576366577316594102531913972535679903434652
c2**(-s) = 104380916181273440540651577574006096437894956727433830312169926979642973225991874377008280886536188561392361725638917874729290605172295208729652998603125917826609388854493499757906714678316256212798276437502202562775736712195054167918488410811225542821934411198105347526230448474593865845934607578391896857144609623981517442857065144480501571172737395368250547626900180521622800929427125523532024089216523419977435765469056906089210477014408038727570233243
```

Коэффициенты: r = 270741, s = 271142
Проверка: 270741 * 1302293 - 271142 * 1300367 = -1
c1r =**
3147537546068979521088581207878527895362018849236245516482550376374187380098103077585520084190879924943634153592341257109358706433230140845960187409082479400263649788392548329667236880004508895337680177299136312764851650283753864717428837514756979729489398243383512833745056805378794703024168535234671850411769843007928065842528124387999030071122408358216248376809397840408228384047544868685317170860623479760080318721582724011840719731242589218461303900473098143544772075069751256763991525485780523370602412926332081883320069986494875157859989300477927205329448906004596470576366577316594102531913972535679903434652
c2(-s) =**
**1043809161812734405406515775740060964378949567274338303121699269796429732259918743770082808865361885613923617256389178747292906051722952087296529986031259178266093888544934997579067146783162562127982764375022025627757367121950541679184884108112255428219344111981053475262304484745938658459346075783918968571446096239815174428570651444805015711727373953682505476269001805216228009294271255235320240892165234199774357654690569060892104770144080387275702332435714460962398151744285706514448050157117273739536825054762690018052162280092942712552353202408921652341997743576546905690608921047701440803872757023324357144609623981517442857065144480501571172737395368250547626900180521622800929427125523532024089216523419977435765469056906089210477014408038727570233243
```
```

5692287629880361126057176578782715045175940819765982347802190113751241968873024035968041159992784033154415543248623211181120249480728911816308731370332435832796

multiplication result =

3285428527736372418032709584516364877889476186907245634768331432120665659255269429524779473894822996640490178798713749032334244213331517903514560434079344217803727015183596846349432690062987558613303489831419200267313510206797531165181876828966866394732683970052401946170538620833533770959936580707942099206622004560540127184488452985461888203070709286480140454307081383183517901674559137049590980431876549298654823163379488806493161015198168318639935530535971996048989823127303097049889794032269409756582892122700504561399209977974893968219191273504932929670261031689331649651639777032859870892970397346762970910385772653538273630769319327511496521702992162052868472589302021802564170574409294405125199606898936545902881811913053032094038296673725569361942088345379858221928235236665517430738359227375343208403007081680151962985913990735744566006884446527642723953080697827901808782451219078120859611974437208765711117477644741073944883994189964404423787590519561942510233806256377588235249936013578518070956831422199482276978182111716588729208986111303319651429085853679608411201110308872289972930346303489538465558793085057698896663654094349016033343728907497487564519801336378885850098560330767986907446072379556193983844469 92

result =

1715057985271786255801963930940868719192886150851291230367229521238518603893308710049109536992701868906086646131906136610407564529465261349366373478533416942493399574884204499116280331727508936092815243522028459491287648209880968810501254307202170621283308860229946165518956868582514605317653854835710803478577583646125967647265964691115925112424219272234607850144440103072945237809832425037272035729853167638103474857915771066589910370744137420983971509906947877982979847230858211140376505809429515911374977414910428567440488176129986698950923214319856149976107082807609792116982183629047507908674091601166139

Расшифрованное сообщение: года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет. информация - сведения (сообщения, данные) независимо от формы их представления;

Вывод: изучил атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.