Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет ИТМО»
Мегафакультет: Компьютерных технологий и Управления
Факультет: Безопасности информационных технологий
Направление (специальность): «Информационная безопасность»
Профиль: 10.03.01 «Комплексная защита объектов информатизации»

Лабораторные работы

по дисциплине

Криптографические методы защиты информации

Тема задания: «Атаки на алгоритм шифрования RSA»

Выполнил:
студент Смирнов М. Г. _____
Проверил:
к.т.н., доцент Михайличенко О.В._____

Дата: _____
Оценка: _____

Санкт-Петербург, 2019 г.

Содержание

1 Атака на алгоритм шифрования RSA посредством метода Ферма

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

Дано: $N = 84032429242009$, $e = 2581907$, $c = 54879925681459721670081829291782821975616617814399744948371366360800117722343426021542724152794267375927192643574021335775875169031132502017752005215695641247980943013$.

1. Вычисляем $n = \sqrt{N} + 1$. В поле A помещаем N, в поле B –2; нажимаем кнопку «D = A(1/B)». В поле D заносится число 9166921. В первой строке таблицы появляется сообщение «[error]». Это свидетельствует о том, что N не является квадратом целого числа.

2. $t_1 = n + 1$. Возводим число t_1 в квадрат: A: = 9166922, B: = 2, C: = 0 (возведение в квадрат будет производиться не по правилам модульной арифметики), нажимаем «D = AˆB mod C» => D = t1ˆ2 = 84032458954084. Вычисляем w1 = t1ˆ2 – N. Для этого A:= t1ˆ2, B:= –N, затем нажимаем «D = A + B» => D = w1 = 29712075. Проверяем, является ли w1 квадратом целого числа: A:= w1, B:= 2, нажимаем «D = A(1/B)» => в первой строке таблицы появляется сообщение «[error]».

3. При вычислении квадратного корня w4 первая строка таблицы остается пустой, а D = sqrt(w4) = r, что свидетельствует об успехе факторизации. t4 = 9166925.

4. Вычисляем p = t4 + sqrt(w4); A:= t4, B:= sqrt(w4), нажимаем «D = A + B» => D = p = 9176129; q = t4 – sqrt(w4) = 9157721. Вычисляем Phi(N) = (p – 1)(q – 1), A:= 9176128, B:= 9157720, нажимаем «D = A · B» => D = Phi(N) = 84032410908160. Вычисляем d, как обратный к e: A:= e, B:= –1, C:= Phi(N), нажимаем «D = AˆB mod C» => D = d = 2475823295643.

5. Производим дешифрацию шифрблока C: A:= C; B:= d; C:= N. Нажимаем «D = AˆB mod C». В поле D находится исходное сообщение M. Переводим M в текстовый вид. Для этого A:= M, нажимаем «D = text(A)». Повторяем с каждым шифроблоком.

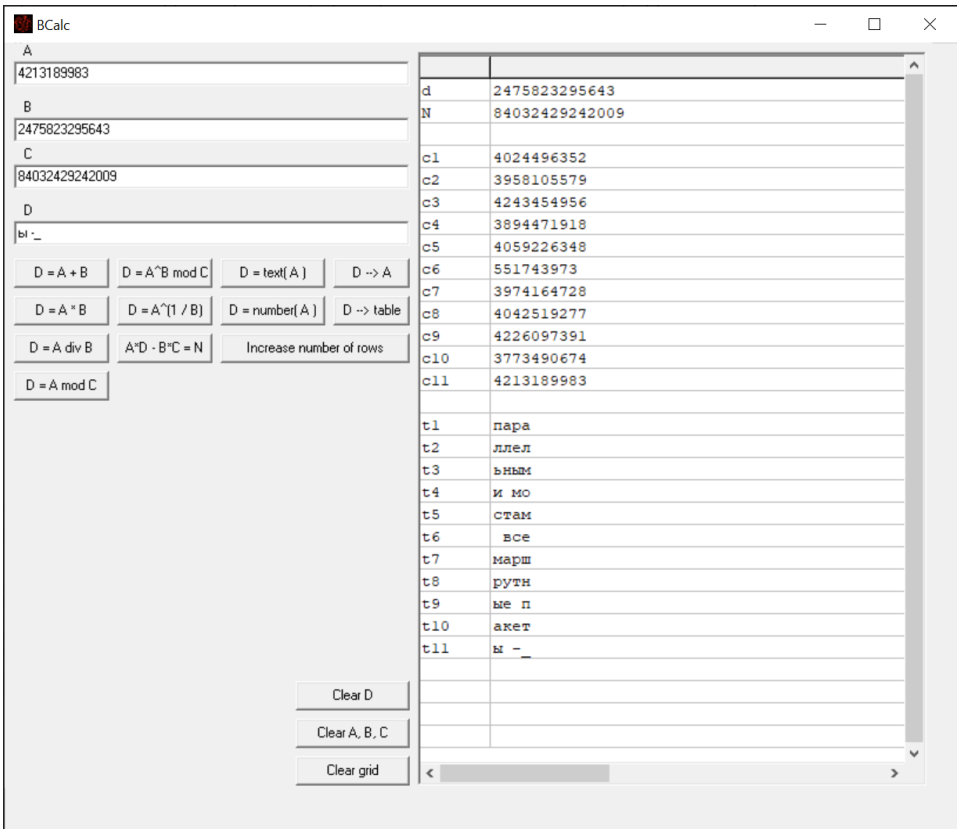

Рис. 1: Результат работы программы BCalc

2 Атака на алгоритм шифрования RSA методом повторого шифрования

Цель работы: изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Исходные данные: $N = 453819149023; e = 1011817; C = 442511634532$.

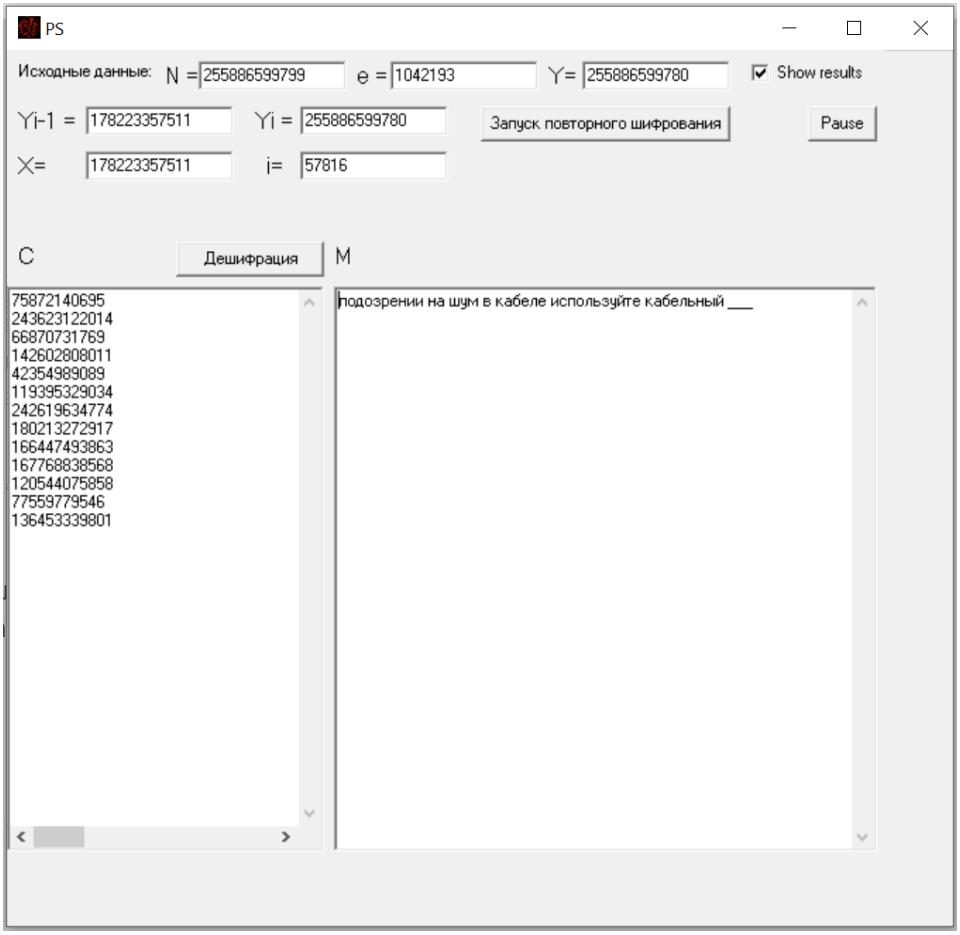

Рис. 2: Вывод программы PS

3 Атака на алгоритм шифрования RSA методом бесключевого чтения

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

Исходные данные: $N = 516439217617; e_1 = 1206433; e_2 = 1141277; C_1 = 400408320444241545246801282223079755490328978748350509811006142356755075109547314116414823859933330990395685377471732609440173195884992413729801710718795 60; C_2 = 37498472136343849130302449895136297721868197485636582720634817504978165635911150546029773474674196963152197362138584797102758207364378173941501204300681 25.$

- Решаем уравнение $e_1 \cdot r – e_2 \cdot s = \pm 1$. Для этого в поле A помещаем значение e_1, в поле B – значение e_2. Нажимаем кнопку «A · D – B · C = N»; C = s = -406030; D = r = 286243

- $c_1 = 400408320444$, $c_2 = 94559770883$

- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $–s$ по модулю N, тогда $c_1^r = 230407699699$, $c_2^{-s} = 32354372535$.

- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r – e2 \cdot s} = 7454696550993853366965$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r – e2 \cdot s)} mod N) = 200458576327$ и преобразуем в текст «»

- $c_1 = 241545246801$, $c_2 = 144847640787$

- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $–s$ по модулю N, тогда $c_1^r = 51618928882$, $c_2^{-s} = 27509250912$.

- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r – e2 \cdot s} = 1419998066423621640384$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r – e2 \cdot s)} mod N) = 82130033820$ и преобразуем в текст «»

- $c_1 = 282223079755$, $c_2 = 236499554090$

- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $–s$ по модулю N, тогда $c_1^r = 259972599441$, $c_2^{-s} = 8867154266$.

- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r - e2 \cdot s} = 230521714417\ 6372365306$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r - e2 \cdot s)} mod N) = 117686786725$ и преобразуем в текст «»

- $c_1 = 490328978748$, $c_2 = 91691946714$

- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $-s$ по модулю N, тогда $c_1^r = 318730996923$, $c_2^{-s} = 306230064232$.

- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r - e2 \cdot s} = 976050136604\ 59684358136$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r - e2 \cdot s)} mod N) = 315058382091$ и преобразуем в текст «»

- $c_1 = 350509811006$, $c_2 = 195676236846$

- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $-s$ по модулю N, тогда $c_1^r = 8257228465$, $c_2^{-s} = 292435110568$.

- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r - e2 \cdot s} = 241470351914\ 7511918120$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r - e2 \cdot s)} mod N) = 100777754363$ и преобразуем в текст «»

- $c_1 = 142356755075$, $c_2 = 105890375451$

- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $-s$ по модулю N, тогда $c_1^r = 133217995591$, $c_2^{-s} = 125953470039$.

- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r - e2 \cdot s} = 167792688163\ 26652598049$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r - e2 \cdot s)} mod N) = 276740551605$ и преобразуем в текст «»

- $c_1 = 109547314116$, $c_2 = 248047563144$

- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $-s$ по модулю N, тогда $c_1^r = 237537182768$, $c_2^{-s} = 342278387913$.

- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r - e2 \cdot s} = 813038439872\ 26683083184$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r - e2 \cdot s)} mod N) = 283204328507$ и преобразуем в текст «»

- $c_1 = 414823859933$, $c_2 = 134557356194$
- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $-s$ по модулю N, тогда $c_1^r = 277612889360$, $c_2^{-s} = 125487085349$.
- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r - e2 \cdot s} = 348368323411\ 00813986640$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r - e2 \cdot s)} mod N) = 190359328241$ и преобразуем в текст «»
- $c_1 = 330990395685$, $c_2 = 223041604801$
- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $-s$ по модулю N, тогда $c_1^r = 47552794481$, $c_2^{-s} = 179282854294$.
- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r - e2 \cdot s} = 852540072420\ 9650351414$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r - e2 \cdot s)} mod N) = 71874538543$ и преобразуем в текст «»
- $c_1 = 377471732609$, $c_2 = 138272971125$
- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $-s$ по модулю N, тогда $c_1^r = 172757639651$, $c_2^{-s} = 10278982505$.
- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r - e2 \cdot s} = 177577275557\ 7723305755$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r - e2 \cdot s)} mod N) = 307737033561$ и преобразуем в текст «»
- $c_1 = 44017319588$, $c_2 = 249978808424$
- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $-s$ по модулю N, тогда $c_1^r = 352291575112$, $c_2^{-s} = 269888526727$.
- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r - e2 \cdot s} = 950794541853\ 11940018424$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r - e2 \cdot s)} mod N) = 201830183707$ и преобразуем в текст «»
- $c_1 = 499241372980$, $c_2 = 344974502483$
- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $-s$ по модулю N, тогда $c_1^r = 17047766454$, $c_2^{-s} = 211271016734$.

- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r - e2 \cdot s} = 360169895178\ 0357841236$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r - e2 \cdot s)} mod N) = 230705485731$ и преобразуем в текст «»

- $c_1 = 171071879560$, $c_2 = 108413221760$

- Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $-s$ по модулю N, тогда $c_1^r = 37543645247$, $c_2^{-s} = 335279611747$.

- После этого результаты перемножаем и получаем, что $m^{e1 \cdot r - e2 \cdot s} = 125876188019\ 81261916509$. Далее берём модуль от полученного значения: $m^{(e1 \cdot r - e2 \cdot s)} mod N) = 201615547888$ и преобразуем в текст «»

4 Атака на алгоритм шифрования RSA, основанный на китайской теореме об остатках

Дано: $N_1 = 420250053679$, $N_2 = 420998138947$, $N_3 = 422793377077$.

c_1	c_2	c_3
17599664694	388099839383	84003082499
221343847340	141363764478	245906362572
181796040962	253757042128	398398702796
210108814452	162556515860	157559004814
124320289825	289849639847	157418944324
323995715057	126598663712	411242039391
260285700707	171600933709	270378838199
72474978285	80576580207	182942084181
226746757036	347679322161	33847193530
369084323018	408725538627	149137845569
133261286623	244886980553	382620866773
336107911000	171682264557	120769412025
303767221006	366784660912	272019119100

Последовательно вычисляем следующие значения:

$M_0 = N_1 \cdot N_2 \cdot N_3 = 138555669564008119302694433926047373$

$m_1 = N_2 \cdot N_3 = 381126913374147389205901$

$m_2 = N_1 \cdot N_3 = 190130221862955939995887$

$m_3 = N_1 \cdot N_2 = 264927981225542872108867$

$n_1 = m_1^{-1} \mod N_1 = 287993142707$

$n_2 = m_2^{-1} \mod N_2 = 106614970676$

$n_3 = m_3^{-1} \mod N_3 = 32171022265$

$c_1 = 17599664694, c_2 = 388099839383, c_3 = 84003082499$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 105147981958387942412346590774900501504511819 99$

$S \mod M_0 = 110624273670950750074744468357233918$

$M = (S \mod M_0)^{1/e} = 480046687691$

$c_1 = 221343847340, c_2 = 141363764478, c_3 = 245906362572$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 292565368798172764575797870873627814465383517 76$

$S \mod M_0 = 405779200391470346741364156381303 87$

$M = (S \mod M_0)^{1/e} = 343634369153$

$c_1 = 181796040962, c_2 = 253757042128, c_3 = 398398702796$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 284936794123323264735894914868840037998118080 50$

$S \mod M_0 = 527756162326213348395123270516146 59$

$M = (S \mod M_0)^{1/e} = 375097731523$

$c_1 = 210108814452, c_2 = 162556515860, c_3 = 157559004814$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 276999655189753875769905936959267078569164320 54$

$S \mod M_0 = 888423116507909009840558604801324 06$

$M = (S \mod M_0)^{1/e} = 446210668924$

$c_1 = 124320289825, c_2 = 289849639847, c_3 = 157418944324$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 208627813962460740292423305916337593177425047 59$

$S \mod M_0 = 321707571739491468694834915826040 26$

$M = (S \mod M_0)^{1/e} = 318043917480$

$c_1 = 323995715057, c_2 = 126598663712, c_3 = 411242039391$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 416336620639102725384464312286213752482727363 48$

$S \mod M_0 = 521563473128696984719117615436486 27$

$M = (S \mod M_0)^{1/e} = 373624823501$

$c_1 = 260285700707, c_2 = 171600933709, c_3 = 270378838199$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 343523785983460037754449318686988869475620311 02$

$S \mod M_0 = 376732649334399111700127116719657 86$

$M = (S \mod M_0)^{1/e} = 335231190925$

$c_1 = 72474978285, c_2 = 80576580207, c_3 = 182942084181$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 111475560955725320312789356130986127555791073 34$

$S \mod M_0 = 719127225262179059034757394980764 67$

$M = (S \mod M_0)^{1/e} = 415848599920$

$c_1 = 226746757036, c_2 = 347679322161, c_3 = 33847193530$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 322243561320241504603319657426319035373733199 34$

$S \mod M_0 = 669361521185193546427950346699732 40$

$M = (S \mod M_0)^{1/e} = 406025753498$

$c_1 = 369084323018, c_2 = 408725538627, c_3 = 149137845569$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 500676770984054905453438966365177747941855874 45$

$S \mod M_0 = 973898358416953880629516893024615 90$

$M = (S \mod M_0)^{1/e} = 460084791933$

$c_1 = 133261286623, c_2 = 244886980553, c_3 = 382620866773$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 228521335723880949630482063790737483230299964 12$

$S \mod M_0 = 118953111957199429876997195076880799$

$M = (S \mod M_0)^{1/e} = 491803863419$

$c_1 = 336107911000, c_2 = 171682264557, c_3 = 120769412025$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 414012982100248963687743955831728403910806527 59$

$S \mod M_0 = 222221761628154428189864985726316 13$

$M = (S \mod M_0)^{1/e} = 281144027527$

$c_1 = 303767221006, c_2 = 366784660912, c_3 = 272019119100$

$S = c1 \cdot n_1 \cdot m_1 + c2 \cdot n2 \cdot m_2 + c3 \cdot n3 \cdot m_3 = 430954908844880462909413503174929482889137376 86$

$S \mod M_0 = 825371726709721609540051429560996 5$

$M = (S \mod M_0)^{1/e} = 202092344693$

5 Атака на алгоритм шифрования RSA посредством метода Ферма

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

Дано: $N = 84920690254116819980017474476393118148268821013112888110434$
$00228686206083816429305891254476516321964070511018025994419860925558186893$
$48729998101602282098438693867582506833766795208024970469782504615932835 5$
$76669396064570181305404758768080305005209944153130165436003818485933486 73$
$33277544321623856347783679869254371677169096401809857942881995328020493 04$
$78963564013572076789009718840237654608474337325427262588758054279994682 48$
$94083865775572170788292771988744018369928165199240564849431076231717152 99$
$79978908200971347370455905740521527289742645433541543472121784179223540 62$
$25913392971814851935883371979117772731283861673, e = 11561117, C = 27606839$
$22915972420219289759000610381217596030907365898849073952843608537473677 00$
$37813503925034009698846392122477248596931626015020066651034980674693651 9$
$00898915427358911897612025255674610054095566225428268760178191475864673 51$
$72423845460427002061777612200240197006451618170451331015817980987204015 01$
$88506260998473827708184953678252898557954311387298338802119127028279839 50$
$20123594968508985128948901911303405382483882174505526077817126810656570 38$
$65420592452710762752343315474601260778725674026769380608444946634676425 37$
$93666668749716689217513724983160321295430932225088571383388154517247768 34$
$07675977287877368705161 50.$

Вычисляем $n = [sqrt(N)] + 1$

A = N, B = 2, $D = A^{1/B} = 29141154790796609743747566801214222187629856907$
$93185242421832742818195600238867601408784089807564080661984396462412014 52$
$28785740299189338334590190389820866601941883471638921663977065798006721 73$
$95575248166874392434687453014189014873271538724919595817010651636073850 00$
$16577015683805052565837087046604039025598 24$

В первой строке таблицы появляется сообщение «[error]». Это свидетельствует о том, что N не является квадратом целого числа.

$t_1 = n + 1$

Возводим число $t1$ в квадрат:

$A = 29141154790796609743747566801214222187629856907931852424218327428$

$$181956002388676014087840898075640806619843964624120145228785740299189338334590190389820866601941883471638921663977065798006721739557524816687439243468745301418901487327153872491959581701065163607385000165770156838050525658370870466040390255982 5$$

$B = 2$

$C = 0$

$D = A^B \mod C = t_1^2 = 84920690254116819980017474476393118148268821013112888110434002286862060838164293058912544765163219640705110180259944198609255581868934872999810160228209843869386758250683376679520802497046978250461593283557666939606457018130540475876808030500520994415313016543600381848593348673332775443216238563477836798693491341484316326367696792323609162882891818766325608811365088727920620660427829598196956096469067001914231713847312429543954001417018840412329762687755621977976425467110638565999100198794155067232638630796559241227735122216750286479750488330297235381840884921062606668844521377162476008780949846833187704030625$

Вычисляем $w_1 = t_1^2 – N$

$A = t_1^2$

$B = –N$

$D = A + B = w_1 = 947624712625362349598212894789209602686888287362044797793011938910901820190174989722618771041804413156177433852629940135567423859801761583052563813353784985159905543054153622891477027078855267443556621083085536668677717001477389053296152914862514163999092685656380755451549562310540125408970729060456420168952$

Проверяем, является ли w_1 квадратом целого числа:

$A = w_1$

$B = 2$

$D = A^{1/B} =$ «$[error]$»

$t_2 = n + 2$

$A = 291411547907966097437475668012142221876298569079318524242183274281819560023886760140878408980756408066198439646241201452287857402991893383345901903898208666019418834716389216639770657980067217395575248166874392434687453014189014873271538724919595817010651636073850001657701568380505256583708704660403902559826$

$B = 2$

$C = 0$

$D = A^B \mod C = t_2^2 = 84920690254116819980017474476393118148268821013112888110434002286862060838164293058912544765163219640705110180259944198609255581868934872999810160228209843869386758250683376679520802497046978250461593283557666939606457018130540475876808030500520994415313016543600381848593348673332775443216238563477836798694074164580132258562571743659633447326644415904484245859849455276484259780475603118478712914430579818046628593139794832448529716223002627179021566495552039310015263136543416999278641514754289502023789127130308026097110028245128316226293565780136427015862188193210306672159924513923486521948367256153995509150276$

Вычисляем $w_2 = t_2^2 – N$

$A = t_2^2$

$B = –N$

$D = A + B = w_2 = 153044780844129454447316423081349404643948542552068184627737848747454094023794851000437558900331722928857431314511234304014313866578554834974436762115020231719874321248693205617101834303898970223470711741683432153805262302985541879983923036470170579802039595780408075876695269907155063857638813838126422528860 3$

Проверяем, является ли w_2 квадратом целого числа:

$A = w_2$

$B = 2$

$D = A^{1/B} =$ «$[error]$»

$t_3 = n + 3$

$A = 291411547907966097437475668012142221876298569079318524242183274281819560023886760140878408980756408066198439646241201452287857402991893383345901903898208666019418834716389216639770657980067217395575248166874392434687453014189014873271538724919595817010651636073850001657701568380505256583708704660403902559827$

$B = 2$

$C = 0$

$D = A^B \mod C = t_3^2 = 84920690254116819980017474476393118148268821013112888110434002286862060838164293058912544765163219640705110180259944198609255581868934872999810160228209843869386758250683376679520802497046978250461593283557666939606457018130540475876808030500520994415313016543600381848593348673332775443216238563477836798694074164580132258562571743659633447326644415904484245859849455276484259780475603118478712914430579818046628593139794832448529716223002627179021566495552039310015263136543416999278641514754289502023789127130308026097110028245128316226293565780136427015862188193210306672159924513923486521948367256153995509150276$

485933486733327754432162385634778367986946569876759481907574466949956577317703970130426428829083338218250478989005233766387604697323920926341790254724322772353531054310289864139457133703033484566420541008059761954325581828307144239368149396234640568109664849342735063459728366432299756186498834914653580066754753276506844970351157846654748033142699291

Вычисляем $w_3 = t_3^2 – N$

$A = t_3^2$

$B = –N$

$D = A + B = w_3 =$ 211327090425722673934811556683777849019208256367931889476174503603818006028572203028613240696483004542097119243759474594471885347176933511643617142894661964923758088191971048945055965899912413702585761375058310640742752905823344854638230781454089743204169922995178076208235583583256115174380554770207203040825 6

Проверяем, является ли w_3 квадратом целого числа:

$A = w_3$

$B = 2$

$D = A^{1/B} =$ 459703263449067407134273506922528075286020339168083978122644550415679608275910529967724835997684762360043583883657702789142275723576286390765907377353309 84

При вычислении квадратного корня w_3 первая строка таблицы остаётся пустой, что свидетельствует об успехе факторизации.

Вычисляем $p = t_3 + sqrt(w3)$

$A = t_3$

$B = sqrt(w_3)$

$D = A+B = p =$ 291411547907966097437475668012142221876298569079318524242183274281819560023886760140878408980756408066198439646241201452287857402991893383345901903898208711989745179623129930067121350232874745997609164975272204699142494582149842464324535497403195585486887640432238367427980482608077614212347781251141637890811

$q = t_3 – sqrt(w_3) =$ 291411547907966097437475668012142221876298569079318524242183274281819560023886760140878408980756408066198439646241201452287857402991893383345901903898208620049092489809648503212419965727259688793541331358476580170232411446228187282218541952435996048534415631715461635887422654152932898955069628069666167228843

Вычисляем $Phi(N) = (p–1)(q–1)$

$A = p–1$

$B = q–1$

$D = A \cdot B = Phi(N) = 84920690254116819980017474476393118148268821013112888110434002286862060838164293058912544765163219640705110180259944198609255581868934872999810160228209843869386758250683376679520802497046978250461593283557666939606457018130540475876808030500520994415313016543600381848593348673332775443216238563477836798691960893675875031823223628092795668364523333408049269650877102404460797201898810881925805074657497726256574007022000865038108627512332920625853950666054196607776822546237065098280818557551653649979315133797249196896824991868948676799112579655955295838204889632585259100775686780909253702045617084519234787420 20$

Вычисляем d, как обратный экспоненте e:

$A = e$

$B = –1$

$C = Phi(N)$

$D = A^B modC = d = 14468764328633144155555109499723048929104078633164036376603635187206837384121210881403998629848933003953520402126579368026163861160975235709280172271790276515412883432200461401418780412189686932343495634382579225199261187753153611244710949843282119225970576521909877529647184047836756960887501093161995825600113491754183544881302938240852551324121256767880412452612035564924979922991544822096326187163303154117865457771234117251366421800008004450642147721797144289264318449084707480193444178299907900478496616222389715722401903940909665094242708308782587585280836401921526412329010450054214463638367782347008364292532 20$

Производим дешифрацию шифрблока :

$A = C$

$B = d$

$C = N$

$D = A^B modC = 18276612538413095939561837092384685844790565701406763781352704781222586972549982184549423772164704977897272453235801304097516895325334345360741184143794550152588743791476884138331380200865981563304009632158378110040846045156997982985694265582543321041946019358954223297139057226517243434451370603262487701903695500130342363377471508869651340689360 20$

608719662246245131174238556398414991606762958162799917576314491449753755973034160550341607206641040036827705128812569462491240420121231156032061778493888517417629187982460589379145535512730513566800235525890007820127375039523278283105089457820683207623444271262303

Ответ: ”технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам”.

6 Атака на алгоритм шифрования RSA методом бесключевого чтения

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

Дано:

$N = 12999302871919244313765393462990170100171107577409215162556252767369383417077598296974306754328982535983925202305207046791609809234141903581786227457426244747553896224664926608868903379245362051127366389409789763449722536283535798325386668928926657067088851933593054098079819666656667022245144869145389688700730235117103691612078891732384120112068808102443661766651503819055747652823937271095614932166906122792265035729741528909213405881670584051440844565239457871084610241717899721985044800816003492162838017178069945951909793500729820463795125504347058156413167604156169328779940912074188119357398453491843442419 13$

$e_1 = 1361953$

$e_2 = 1360027$

$C_1 = 12088343252205973698177879495532558160628407159919598897900358404178513416771114151553436558862570513528584259439782876460111075107403457975420713763599591561617281114708696859472465538975319877743512559006059886374736532091867961955471039099167850332657033795843954349543953032258491203901363222148491195613271905897998400944808165294965913009501612898001171541503440163194822580978042842810607817973439673938102475557024923838836032764707128565956760156893134148300723356238802901468313942361777600847182124122062344034877306087933560979545981654480134659927243673325694450087057858249060039863739686707181557266325$

$C_2 = 36325964996352088027270138369494756332072763271846846119586762292891597434291641511369495230243876744890295157955288129370535694134081572468179363645046558988116451960372069411615883271246572778366814914120801365227788543512211620729324558495427258618372186072305765009838214305302715034245183523214128085228212226911018781118139463294676344735434728488692747458456411691653429430840421600113305878973232852200010542512528272763513962315011931157559677110833867088163283176788434226541575627440732209771108556989122914813897696630323521862316151299817288808932897797684509 14$

594979149328999810032372450514171527644 2

Решаем уравнение $e_1 cdot r – e_2 \cdot s = \pm 1$

$A = e_1$

$B = e_2$

$A \cdot D – B \cdot C = N$

$C = s = 140721$ $D = r = 140522$

$A \cdot D – B \cdot C = –1$

Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $–s$ по модулю N.

$c_1^r = 122124433343250896043011032158937349432203817562148810844733439198317053151077911751580970281014416316060018003049513316362031942447369998310177621845059141924811961499530513611199073572848141703566570077716970575588091639361135048195543640780928116762906387589299016221707279925176001410080510164167520982534104151582461594373558983708565293513461149598943640750223061188920191871708710964973931764148562456092859828401374552872943073240134016287143377740408074312074401808707535357340774593345166617468051299986120867168239118999290891754429881912236213271170713316071715887085405053321588090540013884854317817850302

$c_2^{-s} = 110313785030922927112331345119627217131838694643460236598644623790239780341330760572227854057229292518444736746751871046200950835785618015102950709387212339195438501359606368992471701000194463433664198717391744466399749890750635625056701067281309125826714459655133320701098072148612925977551469396689912520528719354448970815671614405464812742829780238901240086729391814923230925260444836741642485711685014447006244985867065940807582493085601416892365350543627604960515298986219797908403416026242804704599192339691466477840119410209012876267829498577165969211078933419232205704924729204239725198934478237078343377398932

После этого перемножаем результаты и получаем, что $m^{e1 \cdot r – e2 \cdot s} = 1347200848685065549805418502465134553100191945547551508921682490258438323812257685252863892049019976989156398699056675766462134058588231056069316916609871328391195857825840000197307821110046806595985125474834281554406586246804831245427271427645266820406100699600912676416144647441726155778123469929241171907432420346603291838336078079080086661609627219912536550441178816215193945143149554174668722352706122106822532503367399981231845225178482840506952

Решаем уравнение $e_1 cdot r – e_2 \cdot s = \pm 1$

$A = e_1$

$B = e_2$

$A \cdot D – B \cdot C = N$

$C = s = 140721$ $D = r = 140522$

$A \cdot D – B \cdot C = –1$

Производим дешифрацию: c_1 возводим в степень r, а c_2 – в степень $–s$ по модулю N.

$c_1^r = 122124433343250896043011032158937349432203817562148810844733439198317053151077911751580970281014416316060018003049513316362031942447369998310177621845059141924811961499530513611199073572848141703566570077716970575588091639361135048195543640780928116762906387589299016221707279925176001410080510164167520982534104151582461594373558983708565293513461149598943640750223061188920191871708710964973931764148562456092859828401374552872943073240134016287143377740408074312074401808707535357340774593345166617468051299986120867168239118999290891754429881912236213271170713316071715887085405053321588090540013884854317817850302$

$c_2^{-s} = 110313785030922927112331345119627217131838694643460236598644623790239780341330760572227854057229292518444736746751871046200950835785618015102950709387212339195438501359606368992471701000194463433664198717391744466399749890750635625056701067281309125826714459655133320701098072148612925977551469396689912520528719354448970815671614405464812742829780238901240086729391814923230925260444836741642485711685014447006244985867065940807582493085601416892365350543627604960515298986219797908403416026242804704599192339691466477840119410209012876267829498577165969211078933419232205704924729204239725198934478237078343377398932$

После этого перемножаем результаты и получаем, что $m^{e1 \cdot r – e2 \cdot s} = 1347200848685065549805418502465134553100191945547551508921682490258438323812257685252863892049019976989156398699056675766462134058588231056069316916609871328391195857825840000197307821110046806595985125474834281554406586246804831245427271427645266820406100699600912676416144647441726155778123469929241171907432420346603291838336078079080086661609627219912536550441178816215193945143149554174668722352706122106822532503367399981231845225178482840506952

$$5853873600217752714846265334800192237903161716565566555000152715089772474$$
$$3462120950446321488490263306048573167769513203365421393651943361171047403$$
$$6950126970134031711989814134199867883675093769513088239973167431033379627$$
$$1939295989338204815371157124832185219356381886090953561137151087121660940$$
$$2271657798038535454380591525345164164316581050889139298431369195681380413$$
$$2899364628286049764104198260046328582399227672818115806911372190930387350$$
$$8123085827195903267849089645868908746171032422073536017822767776984208169$$
$$4528346003802631879337124799628047491007875705011371508352739166876669148$$
$$8283273014178013153022907494520890943475064061235282174711610682656964807$$
$$0282496636071133302558980912597007696633781465398241484202718666640009069$$
$$6959976257462919211942596447339623887696389538120179 0$$

Далее находим обратное значение по модулю: $(m^{-(e1\cdot r-e2\cdot s)} mod N) = 1752652383$
$$4011375301459908193412802991623654982595821126180572931785172280097964981$$
$$4063445338335392759639631744869717035996621763396869753410738504838820801$$
$$9312951076510427991896407754755207130549401218037374833776972246651238777$$
$$0343615717282236128392166775639177967789975964911825613287722577727696074$$
$$3613118250481577582542426531186352677937948331819750504569641756894020836$$
$$1917046444415191835412524437761677823496205223586990355807338279483286814$$
$$8272942483789083658214636280320858798449795477610689452882790799897335372$$
$$1118269303174144991284042933057091049136793717087732905053034508323792661$$
$$4247927967604575$$

Ответ: ”информация - сведения (сообщения, данные) независимо от формы их представления; информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств”

7 Атака на алгоритм шифрования RSA, основанный на китайской теореме об остатках

Цель работы: изучить атаку на алгоритм шифрования RSA посредством китайской теоремы об остатках.

$N_1 = 17912009682008307506299545034265807505078845780957312788427757923017236749088908831167341406531197617035995249239102277375981357827165610514503837432845571720367326877387011659372151766886605647245389116415880070733767554655197812387624047064028071263462737513248043491964844259093415227255401869822664150863096680176326054913755479830808858724247708186195000273335679757650227564483630445516884196818340413974249484598593155973640963358199655323829982129480889953095302687636409190491500052848690519750150419877656788027501208445665275713027040339197717683210463957207718285878714105987417443525583574122688980729971$

$N_2 = 14064622124792046262850175887962749495676589126365176252374296291320904778604756740222204829477876646644622820371734857059896175099940994412077756063814208974081777712068532688426521682259924752822971129267545623583442948891181467644078660482040124462134048724221174610220018120914283115589657262609674418382288631494709878007673042642813995454933637648009881300930377542232482334869947790747468543156071420583830169504968817366831980330420674435782446297176381271689324560192303415781515725035507838534410598614905942528084555613228030630219707236327979827978582398148814671694992930315805810952071217202862575894057$

$N_3 = 18732132475207488951158085039476341517413149452976800141905283735911675059368828255327933225288665141571137045791108365764511605094676778287064893551904829221478130091400928601885369481539263050441585993357403948008638700041582436182765104957938068173655308254861585399883581469439462625879036589921882061838751390544116837789152223414469000251255180000668858602475863308862938694161390562729714335465980805233844831190960670793553553500275053042574552511370301805661690318710272639305381383552591700177825169933522265175587987556294985109452472983329472874811647165593682375072477678194734406639831760074646991257739$

$C_1 = 29441420234595576629860882117320401635343644305366876991340811793250593478038038501523086069574841536421173316021114105118354894076699998$

541914711614931432324955693814344140493726642722495750077206743906924496098117589765798723779513111022187851135577069873534917622331118150356254741082712591179435855895652909221003751088612785498510995759747238516410600560856247166910982606552406385681864259640212087433171825253497319570254481090872598523079606242323688232849637306045732068863879288582906034399056572126705158161083661203228758788310743456262627867604674727403496243472773761292766815571791471573120609580994915245413204964491594633408566154279464779915078832671713894733364703619536354307209210655474754478427717304432266808783356585217083952364666344088065784213467467023212077432185777015038809212354660598203449662405098898231136714449917151834199531592607265276944668388272612470135663357889115598141751517129709037854850557250953173823748483535996317581930777820653091297629818960109792998035468498753420130835337923153289979705230217375624525490234408636644350032530287243955993974050817902471162381202482144272395760411453526084446884713529790617337907191245352608444688471352979061733790719

C_3 = 1248333924648744582328509345246337248018854199338185258911583418834254222885229599393885488771106012139116569256421841001215238427708566365084267562133358108432868768130928009001699669588210799416767284381766361579883557071817989983577829379436986731244291225552255332570867530130570915934808583936613459495411834651559998089123804105819119676193244832333736065137616884867795205296073266408821917132107152536331693680066137708144248726641521927810966160736808474074745450613007119187207375411698778694268278731011986560459162946298717778144164279324549663035300787612926497616600218837114919581410235419234811759504 5

Последовательно вычисляем:

$M_0 = N_1 \cdot N_2 \cdot N_3$ = 4719104606114270639645920562420444526016050202668827310027103813075033160117032254739581901971836497995246865543247222360004949181498985072038807332192081714015956855525753083791080575861628758937522228699197701850996656644950740693172803481859609305293065552843230525795191787272703646654991410579705576951507805426472998368534398366515491245498115233125786353520460892708243426338027726904499972449892680522388459928445662956389620944575626231415385598834393725181201873244752806995333601642453891282687315649131346996760909226215092809479273829774717410091681860

$$
\begin{aligned}
&2049630838342309634949221866921547314666515220748488793592487984683393451\\
&9182637347126632865618475693613632819527406209162390604392724616331008292\\
&8298163336968187188539212416228331432218686231637975215389299182807655755\\
&7979663024660806232826096577375139808886683158034475076100121539741415766\\
&0146357695270950995603546704169724304455861973654949533200399177660478192\\
&8289961505400386105292747295591429327700120908692933513575301779882162899\\
&6121377429629485109517093913210344485668590159211091202965776020141610380\\
&4713480173196169363553454927670036615769768928024343642762025275500541667\\
&6879765951778110564488769312174990763493181913911226718874170438908369340\\
&4562431125795578865938788773473699841515772302221845533233884716223608412\\
&1264725213324083522107965485077023844440350584241479019036342178120223203\\
&9791999174307041185218324852588758024164200453592419334482375181333501123\\
&4121682741967290673889130587266498105793939570392753019293471578366556724\\
&9592299775602489304534441104763828360691305852988970401559899503994320199\\
&1848288999275975126518243428106777166721742347702029497594687875346992043\\
&6541124277907351358650512574197090373301963323940715433830000039234329663\\
&5858256207984265647464114031859361877296662973874689295468258296678145982\\
&1261410610241848673176786061664257072443343 3
\end{aligned}
$$

$$
\begin{aligned}
m_1 = N_2 \cdot N_3 = &2634603648553388461151460649264088116285306635611196301 2\\
&4843392507913364438005767313436182804233935470975047877777333892222490447\\
&5587366896950619646726698440119206730885802148942184280445482292272931614\\
&1151652685791388292406313874213584355199908709708125245578562119300473688\\
&2099616874919200224537045056881689244798901564984888907772466822336926023\\
&0415041392152546334015383701118255600268396298474800644921234505169795960\\
&2151417465674352182625459484074891364675821339281263351839825502531900925\\
&2981207714256639840455198703989870482554136135770568131702952094108659770\\
&3599912138606770935192353279309723432067272277947384033315073110488291349\\
&0324461780280169763212755882046228350164949380574375437092699135712621080\\
&7608383493360834249070842047330687653546676008322430861808585006233362613\\
&1912911361484525501000578080330594017748594303217173539971264290473540172\\
&2438186166299163706698639967767348176916461709317141876232254434548006796\\
&2664944224740402238792713866906040857414285541369618708882184291481827161\\
&1792695393844872319832679783882136996170906801662208353033806267423614171\\
&7376653401480829756971201013697887147350960615119786103597372780078640342
\end{aligned}
$$

0828546150646058308098287341084350073005819518807383288447075177969087280845357123

$m_2 = N_1 \cdot N_3 = 335530138260578784360593342669543933801227464071798211314930565305691924757863459308220779583058293595319485708300433344165341689602218832231911171759856513118389131583607254865963878536712512517377455010745051275665272009528115935049392976340935490289699136783173212603976607331439271922685074844939881486129463127792864672978736513880772711667064718498948402227940364866860285546712394900890246316524310116672814935476248947267442316850096887444033668375785281027589458867118136296237532617808632418504146123378809928042615829549248325900966396571540381521450310999743964586394432952931191925545454743920074176338279830450994296331190788439443490359641933428923031421903638783802726783897484200677914366702796868298852440660731244841239890464284201264410126346862786907883229253098765821887200243934287132375848925626636339564550307980980187646418875914265860569513507052870598156983217351221883787869450290999203069370417785450844087184849426820047509527891483421803871348049876144965243744110946760865588787403843206150357047681682661325348102205769900363466685582471891648838924556930336743205648204232672083648073197445804699844547019488243554803214844162827347746183833388699607501743287113733125359414011730117053871622995569

$m_3 = N_1 \cdot N_2 = 251925647673063386833666697809979089492792724890938079018256067254492304583016385976161119676781579900233550151107248483340470546386198726859240888466358168945618102663411561777520318399821980645615249802029354817612259615179891436920440211517357260930401618941165074293830626385854612157189477484871086684623735725240541184154194798774755243002418533673294425502217820606925097309782115326428553939053308052779089602959817718408233852317572508039823095670733136345990000572383104807505935676062404332315238654026749255190109427240418880078447729156141036607508144064405391352561313170334616097791338615108559443938333877769163441853700773086943139618140186884597467993849476177113491590231739079947499748651314365026163358545089668213581730731646515277135011583597470768311053874101379196727007502062020549985033624922455907480681894719793381617843590207845793162842078103023707367619398048295259866629553271745639016477815570902312008119478521850336367265426308587318234205191725780510934814393827400806

613282730595100678372944900686488204848453369091783850708589769651841998408102131762262107379143261893032349481668326950465860553288036536894798744402092187946547372383528472950525641014958743040527657967764429123238779820682347

$n_1 = m_1^{-1} \mod N_1 = 1003660185896972911813843680539576308254463929089162725630122667898755883108307805142919440460264317222550270707388548221945257213595850977879975682642606224239945670055909136301835745054490450650676618500552786398320206353764784817733588884217396941936892721834502305696359157091558448132457725469507855838370721026609173677213156137162366537336100167345431179744734148054430559216382545360870349148237541718654181995524555402838799659514923339167363543040013197460136569901360823740479631676025368581414180244956394335583929987400853829394205323642471089470296950405514378434841285984423175859712493409604707708435 7$

$n_2 = m_2^{-1} \mod N_2 = 1153503687784151488078526195486651157958215493998235440929350456057346865426960465428891783217767648050084818302820001767182341166617942400267633070604810583474380764091769166147907830372166100071063775348977607547593076372167788932140401423607426123961466518045297138313802437775583380651025699840548397532280710456682475938484709987433450545818629818099281074953487406996464451313905372597814921002178815905119732436611568211859192519840003221202738061065629727775279640265553521413934250351287248246084885700147909548766274855956217689828837111816928152047165554020686011227318572154818811468037457917153802717049755402068601122731857215481881146803745791715380271704971160505066910726680753649566141598169090240186156138946779857470319569668247842597142578246057654363233275858946132503206350536022868062531336097325245294908987713957888811224199630661342680692441917858571653620647671230569348797064706243853529489029712844477914875678816048316465179991350141772018467316784695846062095942814755953993427934661316004032919797825445596052221246890758110674844768663602527416938428857332746889480845718613003653549039096271397568988103294312145587584840351207273166867869813492874430060989679398013167727332618099167770970402867613615295562502700522158376547815344655868764342064902632 9$

$S = c_1 \cdot n_1 \cdot m_1 + c_2 \cdot n_2 \cdot m_2 + c_3 \cdot n_3 \cdot m_3 = 8124685610241935811863490469911260197783386059111428469737240551748597268316830857041687213353605158199297625602294939132351369946048629717879540206019516318461975642786185898466294 8$

$$
\begin{aligned}
&688743771279612029920205852599974378295567364622123392527896021403656065424259752337434745178828583477177563036972535422469647818324762360622179336419100414969996005757810974464674829421004146752258979246056779182762097374101369133427093855672465373937854567062077363104314702137383259107534808239034618265762580711370178984480595940608422972997701833808183430416381554086117769750506819037963054693981120077855660445394528055504084855387213714532723483938931543164949391167306789462058484899488852983344886420713134697071528120211934048809870934430648206317241695709637888395069217989971151185628580003346571841338818131903675035058772648833580895548909313185512161031880462300550081981339445817680393131983650117230840544594551086123936922870587897452375338487408388298094907617108433667415769175603491112326740273368286573683378040986437168288912520996133502137025344328315121499097961187268253844284437689811095704433651997513413795716897503363239046253657452178669376887455786689345676901911054080281789633848951141488104546501642152461901521288058491020949510662820086682540804616252918699510000625701402883482179594250605345263713503475927910429384926411939981368598423335859549457205759691454725353994456701494910125860529591178714030904400068629822691827778563593102536585117043541773719740372876020304885810627000844448835767195523971461902574543452902480108550313445613773090137352073245958895343429692273593101560573698223415468648561539116599830078699490042547049053623585507683951714860683965781566275133100602785612723632341792386725069755710635469722358656135352721406141582808810460079819443554756433523863128285892589322280010184337188193027303995632678982239119604435874028921136471510671707208676339139125583975948077958426246054533208059933665816691781341447027498630828239920886213094752741451081384388471802643532010512902161292880906929994393741822940776339866062197374846972349674901948010356748280382127873893964102888423598308388061878387130701053129172291626495718499271242619707163861435468134301833984710672365513982170507218340766043912073926763080603395673319360903475928182263726523817255572074402024941102766365787835684299160099534145945053090814529778817153100571086274178006081945659002880593190784434047360851378317104037456046115059553682958 03
$$

$$
S \mod M_0 = 196249357881548562298867002441214325934575881605358992516290466980859998974816593710194009628998020662949095163555649524040486639 7
$$

$$98773521590079172964726786722630454701515788317407431859189753568858269922844787739730924791663009812708596773746686056468170126792869339164652017423233654640131128094965189444873623370452241806548209049066963320191309743411834530318467892149728289622040084076989162250106584025275282683708948928221157816336438138092202356258895850553189251550403417742627015917953719678176448098595443543943201339690530468821400747490442761789262113233769764356657547577047021864647516992926376856259827346268490641113584415198743875861446060529291938092242177563806345789262869999844335869742376510071011531784069981435297558563375305094114019209817616938189131593240253033822373226830035599899210610362312026661555867987339232863657710869443294815178291101078301581490566709668142991043925393132366842715395813497995110058390656229446542964437004814327689478039205934458823775398021970124057936356965865498021345247327056107876321903930706456513488320841666150988463745166873698550821259121509020082286830428353112777969806893174812855316417351524340498692461268256073131214358718056550356125266248834012362747079395746603857699535283295738227752552862150324528234379716045763467792950007133165187984401767569797167018608434490832641045234734349623210500877766418938939431744610175388920640372687403284851193022468105393784065771896689666953308541147886945141842939424903358595058730843527002663170606712916491968586296381079754776304312450329043620529677850394238201521431475433191505305689255471438159983094592884752741900292877151538689285450719638556161525968527095014652075014015749017686905412653892936420014019882099104783930522929073610967674671971886808635104366335512568657441352672889896

$$M = (S \mod M_0)^{1/e} = 26973424141998281784418713363516194232126894235886910455625112052620633847855024302831780630022104506003878091785538925054606842559105353067234863697273452547037908331856516083372454168438755803275452980534770608454108962101440439475470433472094633186925460635281564146672570055907711188133694596996521136941740459544754326680124553955922150401224368772064968911668730019831599376165834814740264563473964185559499075775989250760319675129898967554197465613360027270362395828248920861129140695276903190106200502895903214525066243853944648839597758790172394088833665417090055467574453981780605427068093851116$$

Ответ: ”которых сведения, составляющие государственную тайну, находят свое

отображение в виде символов, образов, сигналов, технических решений и процессов; система защиты государственной тайны – совокупность органов защиты государственной тайны, используем”