

## TAREA-1 Criptografia Híbrida con RSA

- Ramon Gonzalez -

Primero obtenemos los *modulos y el coeficiente* los certificados publicos RSA

```
[rajkit@RAJKIT RUSOS-FINAL % openssl x509 -in bundle_1.cer -text -noout]
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      4b:39:0b:75:64:7a:c1:31:06:40:5a:f0:88:e9:3e:00:69:e7:23:7d
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=RU, ST=Irkutsk, L=Nizhneudinsky, O=belyy medved, CN=Evgeniy Bogachev/emailAddress=Evgeniy@prodikov.ru
    Validity
      Not Before: Oct  2 10:09:23 2022 GMT
      Not After : Oct 12 10:09:23 2022 GMT
    Subject: C=RU, ST=Irkutsk, L=Nizhneudinsky, O=belyy medved, CN=Evgeniy Bogachev/emailAddress=Evgeniy@prodikov.ru
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (1024 bit)
      Modulus:
        00:ca:c9:6f:8c:01:16:b7:11:f5:a2:a6:71:ba:1a:
        55:ec:53:56:c5:57:ac:88:71:c7:54:06:ca:73:34:
        e2:79:ff:92:50:99:5c:6a:8b:cc:01:11:85:99:c9:
        a1:62:37:9e:5f:a7:6e:ae:65:9a:14:9e:54:c9:a9:
        62:57:3f:08:3d:98:42:26:97:8f:18:51:b5:33:14:
        c0:e4:0d:d4:24:b7:c6:5e:26:8d:0f:53:e5:81:6c:
        6c:58:e2:f3:87:7d:71:3e:5f:63:53:44:e1:50:ce:
        0e:98:8c:66:0e:7a:97:54:8e:a7:17:61:03:cc:e2:
        57:30:cc:e9:04:8e:a6:54:05
      Exponent: 5 (0x5)
    Signature Algorithm: sha256WithRSAEncryption
      04:e1:14:03:a1:03:7a:2f:79:44:13:e5:fb:72:03:b0:42:56:
      54:77:e5:69:ca:fa:58:60:77:41:ac:d7:02:67:ea:ab:c9:82:
      32:7f:77:80:42:31:df:86:2f:d9:0d:e5:f3:e1:be:3d:01:56:
      e9:9a:b6:ba:84:a4:ad:2e:30:19:52:09:c5:14:84:2f:03:2c:
      6e:3e:87:7a:f2:d5:57:8c:e1:09:66:23:e1:08:80:9e:c1:af:
      26:24:aa:ad:d2:61:18:b3:f2:48:0a:23:b7:2b:44:69:c1:09:
      e7:4e:9f:58:60:be:a9:2c:de:be:4e:9c:2d:c6:00:fd:15:2e:
      eb:34:
```

Extraemos la llave cifrada con RSA del correo interceptado

```
RUSOS - zsh - 138x49

serial: 488275829382534516586612977085408344298594985512
key_enc_algor:
  algorithm: rsaEncryption (1.2.840.113549.1.1.1)
  parameter: <ABSENT>
enc key:
0000 - 10 eb e8 5c 4a 61 6a d6-2c 6a a1 72 8c 2b 10 ...Jaj.,j.r.+
000f - 0b 32 fd f7 5d 17 09 59-45 d2 39 cb 5d 21 4b .2..].YE.9.]IK
001e - 53 c8 05 92 2b b7 83 4f-e6 00 e0 e4 c4 53 a2 $...+.O..`S.
002d - a2 4d ff 2f b6 d7 69 6c-28 c7 90 74 79 1c ab .M./..il(..ty..
003c - 97 62 ec 33 18 a7 f8 2b-e1 31 a1 18 d2 ad ed .b.3...+1....
004b - c2 73 44 24 6a d9 01 dd-35 8a 64 55 3c 42 d2 .sD$j...5.dU<B.
005a - bb 43 cb 94 e3 e6 07 05-29 56 4f f0 58 2f f8 .C.....)VO.X/.
0069 - 24 3c 44 9c bc 7a 50 25-ca 57 8d 9f 43 34 11 $<D..zP%.W..C4.
0078 - 45 4d 6b 01 a9 52 c7 5b- EMK..R.[

version: 0
issuer_and_serial:
  issuer: C=RU, ST=Irkutsk, L=Nizhneudinsky, O=belyy medved, CN=Murat Urtembayev/emailAddress=Murat@prodikov.ru
  serial: 94624561712435222371373769296598625229713484330
key_enc_algor:
  algorithm: rsaEncryption (1.2.840.113549.1.1.1)
  parameter: <ABSENT>
enc key:
0000 - 6e 9e 75 a3 64 b9 be b0-39 f1 76 81 3b e2 9d n.u.d...9.v.;..
000f - 02 63 09 db 2f a8 a4 98-5c 63 18 ea 2d 71 4d .c../...c.-qM
001e - 6c af 17 a4 2f 60 49 fc-10 5a 2c b7 be 2e 0a l.../I..Z,....
002d - c8 34 ec 45 2d d3 40 d7-85 59 55 16 ef ee 3c .4.E-@..YU..<
003c - 02 87 c4 70 46 fc a6 2f-67 a4 ba d1 7a e2 6d ...pF-/g...z.m
004b - 51 5a 32 4d 47 cb 2f 46-a3 f7 18 a8 3a 50 8a QZ2MG../F....P.
005a - b6 38 54 f4 e5 a4 37 dc-f2 16 42 82 45 76 1c .8T...7...B.Ev.
0069 - 8e 8d b8 ca ae f1 31 19-45 15 da a5 39 63 03 .....1.E...9c.
0078 - e3 a6 e1 be b7 bd f3 49- .....I

version: 0
issuer_and_serial:
  issuer: C=RU, ST=Irkutsk, L=Nizhneudinsky, O=belyy medved, CN=Vladimir Levin/emailAddress=Vladimir@prodikov.ru
  serial: 669925565482167887406315060063283357858094647985
key_enc_algor:
  algorithm: rsaEncryption (1.2.840.113549.1.1.1)
  parameter: <ABSENT>
enc key:
0000 - 16 d7 78 f2 88 ce 3d 0c-6d 95 ab 79 23 9a c6 ..x...=.m..y#..
000f - e4 fc 0d b2 08 ae 03 bf-f0 34 98 09 88 49 9b .....4...I.
001e - 18 2b 7e f4 53 bc 60 85-2b 15 bc a4 3c 9d e2 .+..S..+...<..
002d - 43 bc 6a 3a 38 4f 04 4d-25 8c 31 03 b8 a7 53 C.Z:80.M%.1...S
003c - 55 25 77 cd 0a 7f 9c 08-e0 f9 93 8c 54 b8 a9 U%w.....T..
004b - f2 a8 27 73 0b 5d 73 d6-be bd a8 6b e9 a0 d4 ..'s..l...k...
005a - 2a 99 90 6c 26 81 6d 82-cc 24 a8 e4 91 2a c4 *.l&m..$....K.
0069 - c1 a2 19 69 99 31 3e 37-2f 3f 64 20 0c 6d 30 ...i.1>7/?d .m0
```

Sabemos que la clave **AES-256-CBC** del correo interceptado esta a su vez cifrado con las llaves publicas de los 5 destinatarios, el coeficiente de las llaves publicas es 5.

Deducimos que si se cifra el mismo mensaje *M* con distintas *claves publicas* (*n<sub>i</sub>*, *e*), que difieren en el valor de *n*, pero todas usan *e* = 5, entonces para *i* ≥ 5 y segun el teorema chino del resto es posible calcular *c* = *m*<sup>5</sup> mod *n*<sub>1</sub>*n*<sub>2</sub>*n*<sub>3</sub>*n*<sub>4</sub>*n*<sub>5</sub>, tal que *m* = *c*<sup>1/5</sup>.

```
1 n1=0xcac96f8c0116b711f5a2a671bala55ec5356c557ac8871c75406ca7334e279ff9250995c6a8bcc01118599c9a162379e5fa76eae659a149e54
2 n2=0xDB5EA5970A10A37A9CA9EA29D66E9A0F45C096254B3B3EB14B98BC9CF35BF2519DD19E3A578B5E7EE68A6008E64E7E3FE12D9553B9117D110B
3 n3=0x9F5FE1211DA10A43D03D22343288D8D19E5236F6829633E1FF9379BE4E206053D2B220FF0B5B3A9E042C97FFCC82E8F0B5A512B4083CC91E2
4 n4=0x8C8C7CEED1F3724420F46157540BD4C1D0FA282BB70423494A9AB02691E061FD636EB4D18CBD756FB74D8F3E8D79F83E965EEC3D70563854B
5 n5=0xD853A4C8FEF0915002EC47CF14086699933CBFD5E3A179872CAEC6610EB9572531A7191B949840CBACA791BACFF852C36AB80C90DE5765E426
6 c1=0xBD51A6294C2A7E085CDD995E3C0114DDE3CBA48344AF18EB47E1CEA8901461753A6F75CF5484AEFBDCA953183FD1459CCCF50C2F0F4B4D69DB
7 c2=0x16D778F288CE3D0C6D95AB79239AC6E4FC0DB208AE03BFF034980988499B182B7EF453BC60852B15BCC43C9DE243BC5A3A384F044D258C3103
8 c3=0x10EBE85C4A616AD62C6AA1728C2B100B32FDF75D17095945D239CB5D214B53C805922BB7834FE60060E4C453A2A24DFF2FB6D7696C28C79074
9 c4=0x6E9E75A364B9BEB039F176813BE29D026309DB2FA8A4985C6318EA2D714D6CAF17A42F6049FC105A2CB7BE2E0AC834EC452DD340D785595516
10 c5=0x4154BED91FAB0B74B991283758D311AFE0D3E4970024CD6060716242A57E27CC5ED36D9ACA02AD7FD73C38017CE381853E978F51B20E83DD0F
11 m=crt([c1,c2,c3,c4,c5],[n1,n2,n3,n4,n5])
12 m**(1/5)
13
14
15
16
```

Aplicando el **Teorema del resto chino** obtenemos la clave **AES-256-CBC** con la que esta encriptado el contenido del mail cifrado:

0x3944E0259A49FC5109D63E5E612B9197E7AE016AE8834784BC620D50F264E28F

Procedemos a extraer contenido del mail cifrado para descifrarlo con la clave anterior obtenida, para ello extraeremos tambien el *Vector de Inicializacion* con el que se encripto en modo *CBC*:

```
0078 - d5 de 92 45 5d 10 4a 58- ...E].JX

version: 0
issuer_and_serial:
  issuer: C=RU, ST=Irkutsk, L=Nizhneudinsky, O=belyy medved, CN=Evgeniy Bogachev/emailAddress=Evgeniy@prodikov.ru
  serial: 42944648469846567133467679847969812648301110141
key_enc_algor:
  algorithm: rsaEncryption (1.2.840.113549.1.1.1)
  parameter: <ABSENT>
enc_key:
  0000 - bd 51 a6 29 4c 2a 7e 08-5c dd 99 5e 3c 01 14 .Q.)L~.\..^<..
  000f - dd e3 cb a4 83 44 af 18-eb 47 e1 ce a8 98 14 .....D...G....
  001e - 61 75 3a 6f 75 cf 54 84-ae fb dc a9 53 18 3f au:ou.T....S.?
  002d - d1 45 9c cc f5 0c 2f 0f-4b 4d 69 db 38 55 98 .E..../.KMi.8U.
  003c - 9e c4 96 f1 23 b6 43 cc-1f f8 a8 99 f2 bd 32 ....#.C.....2
  004b - 61 f4 4a 56 d3 d1 14 91-65 1e a8 0b 01 e4 4b a.JV....e....K
  005a - 20 69 57 4a 86 9f 35 fc-eb 67 bf 36 34 ee 33 iWJ..5..g.64.3
  0069 - ce 50 de 74 14 73 74 e9-08 0c e6 e4 bf 37 89 .P.t.st.....7.
  0078 - 25 05 3c c5 d7 f0 9a 4b- %<....K

version: 0
issuer_and_serial:
  issuer: C=RU, ST=Irkutsk, L=Nizhneudinsky, O=belyy medved, CN=Gonzaloff Alvarezosky/emailAddress=Gonzaloff@prodikov.ru
  serial: 637282455933592262985197034165289082024282783775
key_enc_algor:
  algorithm: rsaEncryption (1.2.840.113549.1.1.1)
  parameter: <ABSENT>
enc_key:
  0000 - 41 54 be d9 1f ab 0b 74-b9 91 28 37 58 d3 11 AT....t...(7X..
  000f - af e0 d3 e4 97 00 24 cd-d0 60 71 62 42 a5 7e .....$.`qbB.~
  001e - 27 cc 5e d3 6d 9a ca 02-ad 7f d7 3c 38 01 7c '.^..m.....<8.|
  002d - e3 81 85 3e 97 8f 51 b2-0e 83 dd 0f fe cc e2 ...>..Q.....
  003c - e2 0b 86 c4 5b 86 dd 9f-e9 9c ed e4 04 b8 05 ....[.....
  004b - 4e db d3 fc c8 5f a6 c9-99 7d 74 e6 74 6f 63 N.....}t.toc
  005a - ce eb 34 57 b7 b9 0b 49-5c f4 17 61 e3 d5 b4 ..4W...I\..a...
  0069 - 05 84 9a 75 33 e5 5d 07-1c 4e 1c 34 14 3c 13 ...u3.]..N.4.<.
  0078 - 30 34 70 1d 1a b4 70 7a- 04p...pz

enc_data:
  content_type: pkcs7-data (1.2.840.113549.1.7.1)
  algorithm:
  0000 - 3c 0b 56 09 07 6b 43 c1-e2 f7 37 e2 c8 7e 3d <.V..kC...7..~=
  000f - 09 .
enc_data:
  0000 - 25 5e c1 e1 87 80 37 da-52 1c 5c 60 d0 c9 89 %^....7.R.\'....
  000f - e4 b2 70 fb ea 87 a9 fe-a8 3d 79 3e ee 14 f9 ..p.....=y>...
  001e - 87 92 ..
VECTOR INICIALIZACION
DATOS ENCRIPADOS
```

Con estos datos ya podemos desencriptar los datos cifrados en el correo y obtener el password del certificado que contiene la private-key con el que esta cifrada la clave *AES-128-CBC*

```
Win64 OpenSSL Command Prompt

C:\Users\KERNEL\Desktop>openssl aes-256-cbc -d -in encriptado.enc -iv 3c0b560907
6b43c1e2f737e2c87e3d09 -K 3944E0259A49FC5109D63E5E612B9197E7AE016AE8834784BC620D
50F264E28F
SvobodnayaRossiya
C:\Users\KERNEL\Desktop>
```

Extraemos la *private-key* del certificado:

```
RUSOS-FINAL -- zsh -- 152x58
rajkit@RAJKIT RUSOS-FINAL % openssl rsa -in private-key.key -text -noout
Enter pass phrase for private-key.key:
Private-Key: (2048 bit)
modulus:
 00:be:00:9d:85:35:af:d5:50:c0:79:96:88:f6:4f:
 42:8e:0c:25:03:fd:40:bf:f9:65:4b:62:56:df:8f:
 e2:96:17:da:c0:97:aa:f7:b8:fc:d2:08:0e:4a:db:
 64:e7:96:e5:28:f8:5c:9d:97:61:27:ba:d9:47:b0:
 e2:31:df:b0:c0:2c:0e:ab:d7:74:4b:10:97:89:5b:
 88:c9:f6:b7:bd:e7:43:16:63:7d:07:6a:0a:33:62:
 df:99:01:24:08:bb:0d:bc:5a:f6:c7:46:db:1e:bd:
 ac:ec:33:0a:95:49:89:ab:34:60:76:85:22:ff:39:
 7c:62:01:ef:c5:37:83:ab:14:e9:15:0e:e3:9f:9e:
 e4:dc:4f:68:af:d4:89:81:c7:e9:a0:4a:73:72:df:
 62:f3:bc:ee:ee:ef:21:c7:45:dd:aa:36:4d:0a:a6:
 2e:27:64:bc:c1:02:f9:be:30:35:a7:c6:0c:91:f3:
 80:23:7a:21:91:26:78:c1:f5:ea:d0:0f:cd:9f:9d:
 57:e3:dc:ef:3b:95:d2:85:e6:53:e9:06:8a:35:53:
 f8:f4:01:9f:b7:21:60:ee:86:77:54:d2:e2:7a:47:
 d7:3e:22:16:f4:eb:5b:8b:74:1e:f0:1f:21:4a:37:
 fc:ee:2f:0a:bc:5c:4a:19:0a:ad:cc:b2:bb:97:7e:
 88:95
publicExponent: 65537 (0x10001)
privateExponent:
 00:b6:77:ac:ce:f3:02:0b:df:ea:c7:29:d4:1a:87:
 7f:a9:1e:ec:a5:6a:1f:36:bd:f1:93:75:bb:6c:33:
 a8:2c:f0:77:ba:21:6d:a5:3d:58:3e:f4:51:95:7e:
 20:e7:6f:b8:5f:a2:34:7f:7b:93:08:2e:3e:e9:64:
 74:b5:ea:d6:bf:97:0f:f7:e3:8f:e1:14:eb:08:93:
 b9:48:0b:d1:e5:64:2a:bf:69:07:f7:08:d5:07:08:
 5b:27:7b:3a:f2:20:b1:4e:44:25:5e:b7:23:53:e0:
 60:22:ed:d9:aa:08:d7:57:3d:99:71:14:e6:c9:28:
 91:d5:25:7a:f8:71:19:d7:bf:33:4a:52:87:95:b3:
 66:b8:b6:ab:b5:92:b2:80:af:d6:76:3c:0e:b8:4d:
 49:a8:69:46:aa:58:bd:0c:45:1b:86:9c:03:cf:fd:
 2c:f7:9a:c8:fe:90:1a:d6:a1:f8:bf:73:c1:47:07:
 ee:32:43:31:7e:b6:da:87:e2:ba:f7:75:e5:30:15:
 b1:40:ef:53:50:ea:0c:fe:7d:39:f8:cb:92:55:fa:
 af:0c:b5:11:38:92:19:22:30:4c:e0:fe:98:67:75:
 45:73:a9:3f:c7:01:78:07:b9:43:5b:38:2a:af:
 9f:b7:e5:4f:f6:4a:0b:10:09:1a:50:41:6c:b0:94:
 67:79
prime1:
 00:d5:5e:80:32:20:81:b5:68:fb:f3:76:3f:5c:26:
 0f:17:9b:53:ab:0b:ca:af:0c:c2:07:a2:aa:90:74:
 46:c5:c9:ee:5e:da:eb:81:d7:d1:90:d0:57:e5:f4:
 5d:61:7c:9d:8b:0e:ea:8d:4d:38:d0:7c:80:a1:10:
 d4:9c:ef:78:e3:f8:f4:86:cd:36:81:a4:53:77:50:
 21:0f:44:37:08:b7:6f:dd:94:e5:65:73:83:6c:8a:
 86:7c:05:60:05:d8:94:ab:7a:f5:9a:6f:9f:62:ae:
 74:29:81:4b:34:0c:08:07:cf:fa:14:6e:57:59:3b:
 bf:b2:ca:42:e8:a4:c9:43:eb
prime2:
 00:e3:f6:f1:34:52:90:12:f8:2c:40:f0:bb:73:b6:
 51:e8:78:c3:47:73:af:18:cd:40:62:6b:20:54:29:
 47:93:ac:ef:4e:5d:cd:3f:e0:5a:b4:49:02:81:a8:
 13:89:b9:b7:3d:4e:0e:13:a7:17:48:c2:49:ab:05:
 09:92:2b:75:df:b5:cb:8a:21:ee:55:0e:04:30:66:
```

Extraemos del archivo *encryptedfolder.xml*, todos los datos necesarios, primero los decodificamos ya que estan en *base64*:

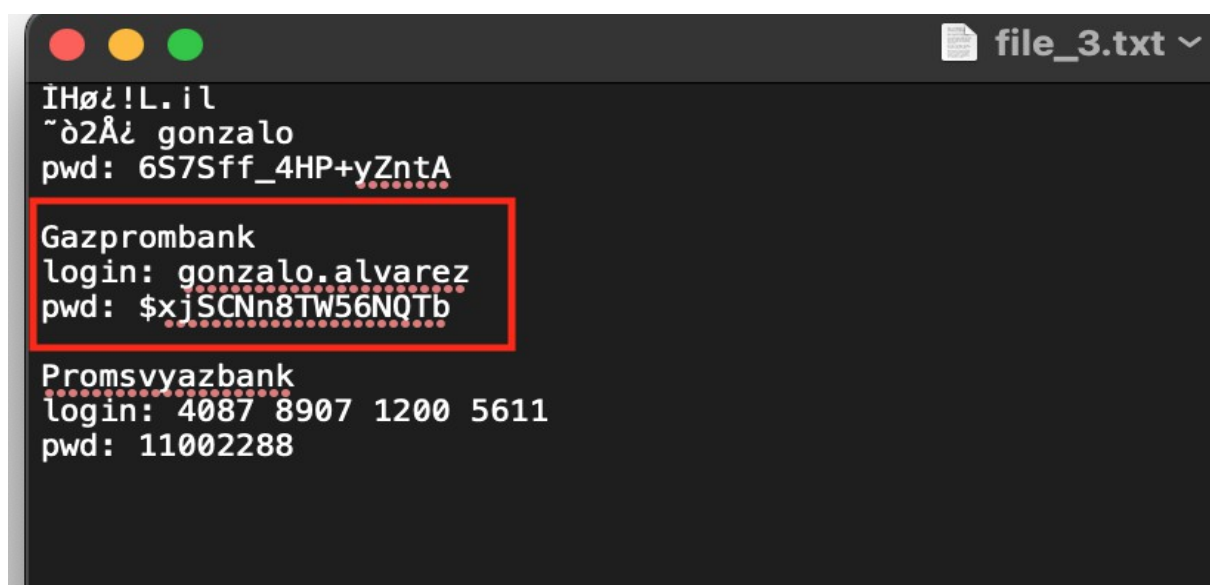
```
23 </file>
24 <file name="File03.txt">
25 <encryptedKey>GZ/aYLr0/wo0zAlEIKzek8ICJsoVXlrjj20ztBSa1juyP+P0Y8u0FbpikTYhk64bB0zsuUjgPqB7b
+FaPVtU8ksrZ0aCjdET2Y9b2e300r9f1xEkmw6wtYQRbGnuQjaNN5Ksa0R1Q7z3nn1FAjA8tbnjIYQfcIlwmrt1CeSi
TAuvWo8Bo/HUQZ42uXe8jktCVrbhJFESHYc0c4z30yeLvSPWHXQbj+jv4yKCLNiESeU89xb9A0KyjxS+uAX8hqHjate
B0xtNiWgYbmdzMMIh4R59VxtWbHsWiLWqaZ0lKTuYYueJqt3AFFwlpzyzskDKDURZkRT5t4DHPCXN8NLV9g==</
encryptedKey>
26 <iv>qPqU04nEVUXCPoINGxwIJQ==</iv>
27 <encryptedFile>aMAaqj zLQ8uaC2ENKIQQ91U1QVFPESDrNxJ2oC2Qbtt8FT3D5hRsg1RuCNxSdr3Evh9w0QzWj cn
fsQSWSLtaVA7oMcHE0L7he3Hhng+VMP7zqdXYqey3+7nmpvG6KLHFcuc3laQJymGv6h9bE4+kIro4qYLFkFmCrNqDr8
SF9kslMbYqinfRkcdCZ+gd5bVde+ncCEPTdJEGBPgecu0K1AME/P96voyayjsEdFtW68=</encryptedFile>
28 </file>
29 </toDer>
30
```

Una vez decodificamos descriptamos la *encrypted-key* con la *private-key* que tenemos:

```
rajkit@RAJKIT FILE_3 % openssl rsautl -decrypt -inkey private-key.key -in file_3.key.enc -hexdump
Enter pass phrase for private-key.key:
0000 - 9e 46 7f c2 7d 93 a5 cf-88 17 77 cb 7e 40 3a 5a   .F..}....w.~@:Z
rajkit@RAJKIT FILE_3 %
```

Con la clave *AES-128-CBC* en mi poder y el *Vector de Inicializacion* procedo a descriptar el archivo FILE\_3.txt.enc

```
rajkit@RAJKIT FILE_3 % openssl aes-128-cbc -d -in file_3.txt.enc -out file_3.txt -iv 16D04E89CAA477000E58E295E447E7DF -K 9e467fc27d93a5cf881777cb7e403a5
a
rajkit@RAJKIT FILE_3 %
```



```
file_3.txt
IHø¿!L.il
~ò2Å¿ gonzalo
pwd: 6S7Sff_4HP+yZntA
Gazprombank
login: gonzalo.alvarez
pwd: $xjSCNn8TW56NQtb
Promsvyazbank
login: 4087 8907 1200 5611
pwd: 11002288
```