Q1 Teamname

0 Points

Cryvengers

Q2 Commands

15 Points

List the commands used in the game to reach the ciphertext.

exit3, exit2, exit4, exit3, exit1, exit4,
exit4, exit2, exit2, exit1, read

Q3 Analysis

60 Points

Give a detailed description of the cryptanalysis used to figure out the password. (Explain in less than 150 lines and use Latex wherever required. If your solution is not readable, you will lose marks. If necessary, the file upload option in this question must be used TO SHARE IMAGES ONLY.)

Using the above commands we have reached the final stage of level and we was given the following details about RSA encrypted password:

You see the following written on the panel:

n =
843644437357250348644025545338262791747038934397633433438632603427566786092168950937792630288092465059556475721766826694452700088164817717014175547688712850204424030016492544050583034399062292019095993486695656975343316520195164095148002658873885392833810539374334969944421464196820276490797049826008575170 93

Cryvengers: This door has RSA encryption with exponent 5 and the password is:

237017877468291103967890949073198303055381803764272832262959065853018895439965334105393817796843668809708962790188071005301766516250869886552108585541333459062725610277

9817144092314796016509489198045275785268570702028938469832266534760990574458224815724693200797833912963006702298796670695548259886980015169 3

We have been given value of n, c in the RSA and value of encryption exponent is given to be 5 i.e $e = 5$. Therefore we know the value of e, c, we need to find value of m. The following relation can be written for the given variables and constants:
$c = (a + m)^e mod(n)$, Where $'a'$ is the number corresponding to the padding.

a is found from the sentence (which we found by the codes given at each exit and by converting them from Hex to the ASCII text),
$"You\ see\ a\ Gold\text{-}Bug\ in\ one\ corner.\ It\ is\ the\ key\ to\ a\ treasure\ f$

(This sentence is converted to integer value by first converting the string into binary and stacking them up and also adding $|m|_{bin}$ zeros at the end).
Padding is assumed to be this because in the sentence it is given that it is the key to the treasure found by. (actually we have added extra space at the end of the sentence after a few trials of strings)

For the encryption part, we have first computed 9×9 matrix using coefficients of functions defined below, K is the upper bound of m and is 2^{64} found after going through the multiples of 8 in the exponent.
Define $R(x) = (a + Kx)^e - c$
For $0 \leq j \leq 4$ the polynomials are $R_j(x) = nK^j x^j$ and
For $5 \leq j \leq 8$ the polynomials are $R_j(x) = (Kx)^{j-5} R(x)$.
The following matrix is then represented from the polynomials as follows:

```
[[c5*(K**3), c4*(K**3), c3*(K**3), c2*(K**3), c1*(K**3), c0*(K**3),       0,     0,
0],
   [      0, c5*K*K,    c4*K*K,    c3*K*K,    c2*K*K,    c1*K*K, c0*K*K,     0,
0],
   [      0,       0,       c5*K,      c4*K,      c3*K,      c2*K,    c1*K, c0*K,
0],
   [      0,       0,          0,        c5,        c4,        c3,      c2,   c1,
c0],
   [      0,       0,          0,         0, N*(K**4),         0,       0,    0,
0],
   [      0,       0,          0,         0,         0, N*(K**3),       0,    0,
0],
   [      0,       0,          0,         0,         0,         0, N*(K**2),     0,
```

0],
[0, 0, 0, 0, 0, 0, 0, N*K, 0],
[0, 0, 0, 0, 0, 0, 0, 0, N]]

Where $c0, c1, c2, c3, c4, c5$ are the co-effecients of $R(x)$.
Now, The matrix is reduced using the LLL reduction using fpylll library.
As known
$R_j(\frac{m}{K}) = 0(mod(n))$ for $0 \leq j \leq 8$ and so the short vector found from the reduced matrix will also have the same property since it is the linear space formed by above basis vectors or polynomials. Also $\frac{m}{K}$ is a root of polynomial formed by short vector as discussed in the lecture.

We have used NEWTON-RAPHSON method to find the approximate root of the polynomial formed by short vector $S(x)$. We have obtained $\frac{m}{K} * K$ as 4773930458381642752, which in binary is '1000010010000000111010000111010101100010010000010110110000000000', which seemed an approximate value of $'m'$ as last eight bits are zeros.
When then decoded the first 7 letters as "$B@hubAl$" and 8th has to be found.

For the 8th one we repeated the above process by taking $K = 2^8$(as we need just last 8 bits) and $'a'$ is the taken correspondingly by excluding the last 8 bits of m and then performed LLL reduction and found short polynomial from it.

The final root obtained from NEWTON_RAPHSON was 33 and so we added 33 to the previously obtained m value to get the exact value of m and thus we got the value of m as 4773930458381642785 and the value in binary is '1000010010000000111010000111010101100010010000010110110000010000001' thus the password is $B@hubAl!$, found by breaking the binary m into 8 bits each and finding corresponding ASCII text.

No files uploaded

Q4 Password

25 Points

What was the final command used to clear this level?