CS641: Level 6

15/04/2021

Reaching Problem Statement

1. There is a maze in which in every screen we can go forward by only one exit while rest of the exits take us back to one of the previous screens. In every screen we see some characters which look like they are in hexdecimal system. We convert them to ASCII and find out that they form a sentence "You see a Gold-Bug in one corner. It is the key to a treasure found by".

$Command$	Hex on screen	$ASCII$
$exit3$	59 6f 75 20 73 65 65 20	'You see '
$exit2$	61 20 47 6f 6c 64 2d 42	'a Gold-B'
$exit4$	75 67 20 69 6e 20 6f 6e	'ug in on'
$exit3$	65 20 63 6f 72 6e 65 72	'e corner'
$exit1$	2e 20 49 74 20 69 73 20	'. It is '
$exit4$	74 68 65 20 6b 65 79 20	'the key '
$exit4$	74 6f 20 61 20 74 72 65	'to a tre'
$exit2$	61 73 75 72 65 20 66 6f	'asure fo'
$exit2$	75 6e 64 20 62 79	'und by'

2. On the last screen we proceeded by "exit1" and got no hexadecimal text and couldn't proceed using any exit. So we used "read" command here and gor the following:
$n = 84364443735725034864402554533826279174703893439763343343863260342756678609216895093779263028809246505955647572176682669445270008816481771701417554768871285020442403001649254405058303439906229201909599348669565697534331652019516409514800265887388539283381053937433496994442146419682027649079704982600857517093$

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

$237017877468291103967890949073198303055381803764272832262959065853018895439965334105393817796843668809708962790188071005301766516250869886552108585541333459062725610277981714409231479601650948919804527578526857070202893846983226653476099057445822481572469320079783391296300670229879667069554825988698001516 93$

Analysis

In RSA encryption and decryption we have:
a. Encryption: $C = M^e mod N$
b. Decryption: $M = C^d mod N$

For decryption we see that N is 1023 bits long so it is impossible to find it's factors.
We cannot compute d, but as N couldn't be factorized and so we cannot find $\phi(N)$.

Now, as the public exponent is small we apply low-exponent attack, the Coppersmith's Algorithm.

Decryption using Coppersmith's Algorithm

This algorithm requires a polynomial as an input. Thus, we need to formulate the same. For this, we

first need to check if any padding is added to the Message. This can be done by checking if $C^{1/e}$ is an integer or not.
We computed the same and found that padding is added. Let x be the padding, thus final equation becomes: $(x + M)^e = CmodN$
In the above equation e, C, N are known. We will try to guess x as Coppersmith says that if we are looking for $N^{1/e}$ of the message, it is then a small root and we should be able to find it pretty quickly.
Coppersmith's Theorem: Let N be an integer and f be a polynomial of degree . Given N and f, one can recover in polynomial time all x_0 such that $f(x_0) = 0modN$ and $x_0 < N^{1/}$.

So, we can form the problem as follows

$$f(M) = (x + M)^e modN$$

For solving this, we use $SageMath$ for algorithms required as it has built in $fplll$ library in it.
To start off, We need to be given a major part of the message x and we need to find $M < N^{1/e}$ which is the password. In the question we are provided with two strings:
a. "You see a Gold-Bug in one corner. It is the key to a treasure found by"
b. "Cipher: This door has RSA encryption with exponent 5 and the password is: "

The length of password M from our assumption is less than $N^{1/e} \approx 4 * 10^{61}$ thus, M can't be longer than 206 bits. So, we get our polynomial as,

$$f(M) = ((binary(x) << length(M)) + M)^e - C$$

Root of the above polynomial is the required password which is calculated using Coppersmith's Algorithm and LLL (Lattice reduction).

Result

The root found by the modified Coppersmith's Algorithm was found with string "You see a Gold-Bug in one corner. It is the l
which is :
00100000010000100100000001101000011101010110001001000001011011000010000 1

Now, we picked 8 bit blocks at a time and decoded using their corresponding ASCII value and the decrypted password found out to be:
"$B@hubAl!$"
Full sentence found is: "You see a Gold-Bug in one corner. It is the key to a treasure found by B@hubAl!"