CS641

Modern Cryptology

Indian Institute of Technology, Kanpur

Group Name: Cryptomaniacs

Vishesh Kaushik (170805), Tarun Kanodia (190902), Kaustubh Verma (190924)

Assignment 6

Submission Deadline:
April 18, 2022, 23:59hrs

Question 1

You see the following written on the panel:

$n = 84364....600857517093$

Cryptomaniacs: This door has RSA encryption with exponent 5 and the password is 27988....043.

Solution

Reaching the question:

To reach the question, we saw the hex values provided at the end of screens after taking an exit, and converted them to corresponding ASCII characters. They seemed to be forming a sentence. We kept following different screens by hit and trial, while also simultaneously creating a **DFA**, which ultimately led us to the screen where the sentence completed as: **"You see a Gold-Bug in one corner. It is the key to a treasure found by "**. At this screen, any of the exits lead us to states that were already visited, and hence we knew this was the end screen, and doing read on it revealed the question.

Cryptanalysis:

It is given in the assignment that $e = 5$. We have assumed that the actual message m is padded with some some padding a such that $c = (a + m)^5 (\text{mod } n)$. We have constructed a polynomial $R(x) = (a + Kx)^5 - c$ where K is an upper bound on m(we have taken $K = 2^b$ where b is the number of bits in m). We can see that $R(x)$ has a "small" root in Z_n

since $R(m/K) = 0(\text{mod } n)$ and $m/K \leq 1$.

As discussed in the lecture, we defined 7 polynomials of the form $R_j(x)$ for $0 \leq j \leq 6$ as : $R_j(x) = nK^jx^j$ for $0 \leq j \leq 4$, $R_5(x) = R(x)$ and $R_6(x) = KxR(x)$. Every R_j satisfies the property that $R_j(m/K) = 0(\text{mod} n)$. We defined vectors $v_j \in Z^7$ for each of the polynomial to contain the coefficients of polynomial R_j. Let L be the lattice generated by vectors $v_j, 0 \leq j \leq 6$ and let $R(x) = K^5x^5 + c_4K^4x^4 + c_3K^3x^3 + c_2K^2x^2 + c_1Kx + c_0$. Then we get volume of lattice as follows:

$$v(L) = \begin{vmatrix} K^6 & c_4K^5 & c_3K^4 & c_2K^3 & c_1K^2 & c_0K & 0 \\ 0 & K^5 & c_4K^4 & c_3K^3 & c_2K^2 & c_1K & c_0 \\ 0 & 0 & K^4n & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & K^3n & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & K^2n & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & Kn & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & n \end{vmatrix} = K^{21}n^5 \tag{1.1}$$

We have used the Lenstra-Lenstra-Lovasz (L^3) Algorithm to find the short vector $u \in L$ and we have $|u| \leq 4\lambda_1(L) \leq 4\sqrt{7}K^3n^{5/7}$ where $\lambda_1(L)$ is the length of the shortest vector . Let $S(x)$ be the polynomial whose coefficients are given by vector u. Since S is an integer linear combination of R_j's, $S(m/K) = 0(\text{mod } n)$. Also,

$$|S(m/K)| \leq 28\sqrt{7}n^{5/7}K^3 < 2^7 2^{192} 2^{732} < 2^{931} < n \tag{1.2}$$

which means $S(m/K) = 0$ over Z(assuming K is atmost 64 bits long). We calculated the approximated value of roots using *polyroots* function present in python. These approximation can be multiplied by known value of K to obtain the closest integer to the result which gives the value of m'. If any of these m' satisfies the condition $(m')^e = (a+m)^e = 0(\text{mod } n)$ then that m will be the actual password and the same thing happened, we got one m which satisfied the above condition. As we knew the padding, we got the value of the actual message m which is also the password for this assignment.

How did we find the padding?

To find the padding, our first instinct was to use the sentence that had led us to the question screen. The sentence was: **"You see a Gold-Bug in one corner. It is the key to a treasure found by "**. We tried this to be the padding in our code, but we were unable to

find any roots for the polynomial. After some hit and trial, we tried the question which was on the screen as padding, which was: **"Cryptomaniacs: This door has RSA encryption with exponent 5 and the password is "** and using that gave us the root (in binary):
01000011 00111000 01011001 01010000 00110111 01101111 01001100
01101111 00110110 01011001. Using each 8 group of bits as numbers and looking at corresponding ASCII character gave us **"C8YP7oLo6Y"**, which was the password. Also we have $a + m$ as **"Cryptomaniacs: This door has RSA encryption with exponent 5 and the password is C8YP7oLo6Y"**.

Note: Not using space at the end of the padding gives a different root, which on converting to ASCII gives **" C8YP7oLo6Y"** as the password, both of which work on the right screen.