CS641A: Assignment 7

Rijndael

Abhishek Jain, Arham Chopra, Ayush Tulsyan

13027, 14130, 14807167

1 The Maze

You are in a small chamber. Unlike the previous hall, this chamber seems naturally formed – the floor and walls are rocky and uneven. Was that hall and pool an illusion, you wonder. But then you notice a sign of human (or whatever) work: that someone has fixed lighted torches in the walls of the chamber, and these are providing ample light to see around. So you were not dreaming after all..
You then notice that there are several exits from the chamber. You count five. And all but one of these exits have no doors! The exit with door has a panel next to it and the door is closed. Going closer to an open exit, you notice "Exit 2" written on the wall next to it. Curious, you go around and find that the exits are numbered from 1 to 5 in this fashion. The closed exit is numbered 5 and the exit from which you came in is numbered 1.

$>exit2$

You reach a chamber that has five exits, numbered one through five. Exit numbered five is closed with a panel next to it. Remaining are open.

$>exit4$

You reach a chamber that has five exits, numbered one through five. Exit numbered five is closed with a panel next to it. Remaining are open.

$>exit3$

You reach a chamber that has five exits, numbered one through five. Exit numbered five is closed with a panel next to it. Remaining are open.

$>exit1$

You reach a chamber that has five exits, numbered one through five. Exit numbered five is closed with a panel next to it. Remaining are open.

$>exit4$

You reach a chamber that has five exits, numbered one through five. Exit numbered five is closed with a panel next to it. Remaining are open.

$>exit4$

You reach a chamber that has five exits, numbered one through five. Exit numbered five is closed with a panel next to it. Remaining are open.

$>$*exit2*

You reach a chamber that has five exits, numbered one through five. Exit numbered five is closed with a panel next to it. Remaining are open.

$>$*exit2*

You reach a chamber that has five exits, numbered one through five. Exit numbered five is closed with a panel next to it. Remaining are open.

$>$*exit1*

You reach a chamber that has five exits, numbered one through five. Exit numbered five is closed with a panel next to it. Remaining are open.

$>$*read*

**n=765321869214839257303335428604719475698016458049270044398448515508800963 1
15925765931056864437990494467975778411738226986462673134171660866648158943 4571992
19733238098389453856039769503972948608426467982630775728004335548405189781 5167503
66528123913784895902196840820310276388921386050770681516045170375330120 09**

**Rijndael: This door has RSA encryption with exponent 5 and the password
56789403245619791465269992625908733575606033360556986669402092071949485662541847654
0582987491710901019141026294584346841796558095302411963454123118862443276179903 13
0795185831598976614511037949456628955047956219020366928934496604454598971006866 81
609714620951109230397159280735062902807247528481800505391665 57**

The cipher is efficiently decrypted through the following function

$$dec(C, d, N) = (C)^d mod N$$

but d is unknown. Also, d might be as 1000 bits long. So, guessing d is not possible.

Now, with the small public exponent, it is apparent that a low-exponent attack has to be used.

Trivially, we proceeded with checking if no padding has been used and $C^{\frac{1}{e}}$ is an integer, but this is not the case.

With a padding the equation becomes

$$(M + x)^e = C \ mod N$$

In this equation, e, C, and N are known. We can also guess M (which we discuss later). Thus low exponent attack can be used here [2].

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 $f(x_0) = 0 \; modN$ and $x_0 < N^{1/\delta}$ [1]

Now, with this hand, we model our problem as follows $f(x) = (M + x)^e \; modN$. If x is smaller to $N^{1/e}$, we will find the required password as the root to this polynomial

For solving this polynomial we used the a code available on github[3]. This code can be used to obtain the solutions for the polynomial equation modulo N. We modified the code as follows:

1. It demonstrates the attack over two setups. The second is irrelevant to us, so we got rid of that
2. N, e are known to us
3. To test the code, we used a custom message, generated the cipher C and and a random password for x. Verified that the code works
4. Now we started with a custom padding `M`, translated it to its binary form `M_binary`
5. The length of password x is unknown, but since ascii has been translated to binary, we assume it to be a multiple of 8. Also, from our assumption $x_0 < N^{1/e}$, x can't be longer than 200 bits. So, this can guessed via brute force
6. The final polynomial is $pol = ((M\_binary << length\_x) + x)^e - C$
7. Root of the above polynomial is the required password and can be calculated using Coppersmith's Theorem and LLL (Lattice reduction)
8. For trying random input paddings, we changed the code to read from a hardcoded file "paddings.txt", and try each line as the padding.
9. We also changed to the working coppersmith to a function so that it can be called with different parameters.

Random and Not so obvious Padding, M

For the M, we tried quite a few values.
Some examples being:

- "You reach a chamber that has five exits, numbered one through five. Exit numbered five is closed with a panel next to it. Remaining are open."
- The combined string of all our passwords from previous assignments till now in serial order
- Rijndael: This door has RSA encryption with exponent 5 and the password is
- RIJNDAEL: THIS DOOR HAS RSA ENCRYPTION WITH EXPONENT 5 AND THE PASSWORD IS
- rijndael: this door has rsa encryption with exponent 5 and the password is
- This door has RSA encryption with exponent 5 and the password is
- Indian Institute of Technology, Kanpur
- CS641A: Modern Cryptology
- Rijndael: This door has RSA encryption with exponent 5 and the password is:

Before the last one we tried quite a few more(read hundreds).
Then we tried randomizing the last characters of the above strings and we got a hit with the last line.

The password we got was `JBILKLNLKQ`

References

[1] J.-S. Coron. Universite du Luxembourg Cryptography, Lecture Slides: Attacks against RSA, 2010. URL: http://www.crypto-uni.lu/jscoron/cours/mics3crypto/cop.pdf. Last visited on 2018/04/22.

[2] J. Dyer. Lattice reduction on low-exponent rsa, 2002.

[3] D. Wong. Rsa-and-lll-attacks. URL: https://github.com/mimoo/RSA-and-LLL-attacks/.