jamk.fi

Final Report

Encryption Techniques and Systems

Jere Pesonen, M3227

RSA vulnerabilities
12-2020
Information and Communication Technologies

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Contents

1 Introduction

After doing the course assignment of RSA algorithm, implementing my own one, and studying it's works and modes of operation. I think the natural continuation is to get to know the vulnerabilities that may occur. In this document I'm doing a research about the common vulnerabilities, that appear in RSA algorithm implementations and what may cause them.

RSA: s security is based on the mathematic operation, that uses large randomly generated prime numbers. It has been considered the most consistent algorithm used in message encryption because it has truly passed the test of time. Since it was introduced back in 1977, to this date no one has been able to come up with a profitable solution to cracking it. The method for the cracking will require an efficient way to divide large numbers into factors to figure out the prime numbers behind the private key. That being said, the vulnerabilities are not going to be in the mathematic operations, they are going to be in the implementation. I'm going through the mistakes in the implementation that can break the algorithm, their causes and consequences. I am assuming that reader of this is familiar with basic mathematic operations of RSA algorithm. (The Reliability of RSA Encryption Research Papers Examples. 2020)

2 Unsecure key generation

First choke in the RSA implementations is the usage of low keys. It means that the any of the necessary integers generated (or chosen) for algorithm is assigned to too small. RSA: s security is based on large integer keys, and their relative operations, and cracking them takes time even with powerful computers. Small key usage creates vulnerabilities in the math system, and it makes reversing the operations a lot easier. It might be tempting to do this, for easing the load of the operation and making it faster. (If the environments hardware can't handle large digits. (fuck-rsa 2019.)

2.1 Too low modulus

The length of the RSA keys makes a major difference in the security. Since it can all be figured out with mathematic operation, it should not be to short, when the calculation can be run through in reasonable time. 1028-bit key is commonly used, and its good enough, so the counting operation would need so much recourses, that it would not be worth it anymore. Shorter than 1028-bit keys are not recommended, and 2048-bit key is considered not to be vulnerable for brute force attacks at all. (Attacking rsa. 2020)

2.2 Low public exponent

When public exponent is assigned as too low of an integer, it exposes the algorithm to the various attacks. The common one in this case is Hastads attack, or Broadcast attack. In Hastads attack, the attackers need to get hands to multiple ciphertexts, which have all encrypted the same plaintext with same public exponent. Amount of the ciphertexts needed is equal to public exponents number (smaller public exponent, easier decryption). When attacker has the needed quantity of public key – ciphertext pairs, he can use the Chinese remainder theorem, to count the encrypted plaintext. Chinese remainder theorem is an operation to figure out the remainders between multiple given numbers and their divisors. (Attack on RSA with Low Public Exponent. 2004)

2.3 Low private exponent

Private exponent is used when decrypting the ciphertext. If the private exponent is smaller than fourth root of the key N, the attacker can figure out the key. The most famous small private exponent attack is called Wieners attack. It is based on approximations on the continuous fractions. In Wieners attack, the private key d can be reversed by calculating the right $\frac{k}{d}$ among the convergents of $\frac{e}{N}$. (Attacking rsa. 2020)

3 Coppersmith attack

Coppersmiths attack is bunch of attacks that can be used against a public key exponent, or in a situation where a part of secret key is available. I found two examples where first one attacks the prime number p used in the key generation, and second one uses partially know message. (Coppersmith attack. 2020)

3.1 Partially known public key

First method is to figure the factoring with some known bits of the factors of public key. The attack uses pretty complicated mathematic operations to calculate whole integer from just partial of it, but if the operation solution is a factor for public key N, the private key is easily calculated. (Latticehacks RSA. 2020)

3.2 Partially known message

Second method uses partially known message to figure the unknown one. For example, if password encryption uses padding of some kind, and the padding is known, it can be used to calculate the password, that is included in the same string. (Latticehacks RSA. 2020)

4 Conclusion

The vulnerabilities stated are just some examples, of what kind of problems you might face when using or implementing RSA algorithm. Internet offers a huge load of different algorithms and systems that can be used to cracking the encryption. Common, they use a vulnerability by unsecure keys, so these are as well caused by the hick ups in implementation.

One big concern in the future, that is going to affect the 100% safe RSA, could be quantum technology. It’s expected to have the calculation capacity of breaking a 2048-bit encryption in 8 hours. is expected to break the algorithm

5 References

Attacking rsa. Writing in sjoerlangkemper.nl website. Sjoerd Langkemper. Referenced in 7.12.2020. https://www.sjoerdlangkemper.nl/2019/06/19/attacking-rsa/

Attack on RSA with Low Public Exponent. Lecture material from Tel Aviv University. Ishay Haviv. 2004
https://cims.nyu.edu/~regev/teaching/lattices_fall_2004/ln/rsa.pdf

Coppersmith attack. Wikipedia article. N.a. Referenced in 7.12.2020

https://en.wikipedia.org/wiki/Coppersmith%27s_attack

fuck-rsa. Blog writing in trailofblits.com. Ben Perez. 8.7.2019.
https://blog.trailofbits.com/2019/07/08/fuck-rsa/

Latticehacks RSA. Web page of RSA Attacks. N.a. Referenced in 7.12.2020
https://latticehacks.cr.yp.to/rsa.html

The Reliability of RSA Encryption Research Papers Examples. Research Paper in woweassys.com website. Writer ID 128768. 29.3.2020
https://www.wowessays.com/free-samples/the-reliability-of-rsa-encryption-research-papers-examples/

Twenty Years of Attack on The RSA Cryptosystem. Document in Stanford.edu website. Dan Boneh. Referenced in 7.12.2020.
https://crypto.stanford.edu/~dabo/pubs/papers/RSA-survey.pdf