Cryptology: Security in RSA Public Key Cryptosystem

hi@almb.me

It's undeniably true that RSA is the most popular public key cryptosystem used today which provides security and privacy of digital information. There are many types of Public Key System (PKS) but only few of them gained mainstream usage as pointed out by Bruce Schneier, RSA, ElGamal, and Rabin [Bruce Schneier, 1996]. As of today there has not been a practical truth that RSA has been broken. Meaning, we can continue to use RSA as long as we choose higher prime numbers. RSA today is used in web Servers, web browsers to ensure the authenticity and privacy of the information transmitted over the internet. In this paper, we looked at the history of attempted attacks to RSA function.

Before discussing the attack on RSA, let point out that the main idea of a cryptographic attack is to be able to gain knowledge of the plaintext regardless of which stage or round of braking. Based on the methodology used, attacks on cryptosystems are categorized as follows: Ciphertext only attack (COA), Known Plaintext Attack (KTA), Man in Middle Attack (MIM), Chosen Plaintext Attack (CPA), Dictionary Attack, Brute Force Attack (BFA), Birth Attack, Fault analysis Attacks, and with most prominent one such as Side Channel Attack (SCA), Timing Attacks, Power Analysis Attacks.

To understand the security of RSA, the approach is to learn different attacks performed to break the RSA PKS and why we have a new scheme of PKS. Such as the Elliptic Curve Cryptography. A number of groups of researchers today, as mentioned by Don Boneh in his paper "Twenty Years of Attacks on the RSA Cryptosystem", although twenty years of research have led to a number of fascinating attacks, none of them is devastating. We can totally argue that there is always a flow in every system designed, however, RSA is still proven as the most secure PKS cryptosystem designed by far.

In 1977, it was mentioned that the difficulty of breaking the RSA cipher is connected to the difficulty of factoring large numbers. In August 1977 the RSA inventors published a challenge to decode the cipher text. This challenge appeared in Martin *Gardner's Mathematical Games column* issue of Scientific American. It was solved in 1993 thus the famous quote of the plaintext itself **"The Magic words are Squeamish Ossifrage".**
Historically, at the time there wasn't enough computing power, and there were over 600 volunteers who contributed CPU time from about 1,600 machines, two of which were fax machines. This is important to note because it requires an enormous computing power to break a cryptosystem. The decryption of the 1977 ciphertext required factoring a 129-digit, that's about 426bit, to gain the plaintext.

As we study the composition of RSA, weaknesses are studied in two approaches: the RSA function and RSA Cryptosystem. Dan's studies focussed on the RSA function. As known from its basic mathematical composition:

$$\text{Let } N = pq,$$

the product of two large prime numbers of identical size (n/2 bits each). Now, let N be the RSA modulus, e the encryption exponent and d the decryption exponent, The pair (N,e) is the encryption and the pair (N,d) the decryption which is the private key known only by the recipient of the encrypted message. A legitimate decryption of the messenger, the user would compute

$$C^d = M^{ed} = M(\text{mod } N),$$

Referring to the RSA function definition, if d is given, the function can be easily inverted using the for equality. The iverstion of the RSA function is what Dan refers to as breaking RSA. Furthermore breaking the RSA function is not symmetrically the same as breaking the RSA cryptosystem. Cryptosystems built around RSA are mostly subtle to most attacks but only their implementation

The attacks on cryptosystems described here are highly academic, as the majority of them come from the academic community. In fact, many academic attacks involve quite unrealistic assumptions about the environment as well as the capabilities of the attacker. As found on the RSA attack, pointed by Dan, the two decades investested into attacking the RSA cryptographic function has only proven some insightful advancement on attack methodology but these attacks only illustrate the pitfall of bad implementation of RSA which can be avoided during its implementation.

Although there has not been a proven practical known breakthrough attacks of the RSA PKS, we have seen strong development of acclaimed faster PKS such as the Elliptic Curve with many variants. The known curve widely used in cryptosystem is the Curve25519, more specifically used in the Elliptic Curve Digital Signature algorithm (ECDSA).

In conclusion, the RSA cryptosystem is still resistant to most attacks as long as it is carefully implemented. For example, if you use the SSH (secure shell protocol) service, use a higher number to generate the SSH key such as 2048 or better off 4096.

References

Boneh, Dan. *Twenty Years of Attacks on the RSA Cryptosystem*. Notices of the American Mathematical Society (AMS), Vol. 46, No. 2, pp. 203-213, 1999

R.L. Rivest, A. Shamir, and L. Adleman. *A Method for Obtaining DigitalSignatures and Public-Key Cryptosystems.* February 1978. http://people.csail.mit.edu/rivest/Rsapaper.pdf

Schneier, Bruce. Applied Cryptography. Second Edition, 1996