Are prime numbers the key to modern encryption? (Kai Parker Lx5)

Millions of prime numbers have been used to protect online transactions by the RSA cryptosystem. This cryptosystem, a system of algorithms used for security, is based on the ideas of notable mathematicians: Gauss, Fermat and Euler. However, technological and mathematical advancements may be detrimental to global security as they threaten to break the system. These include quantum computers' vast computation power in addition to developments around the Riemann hypothesis. It is a problem yet to be proven despite being over 150 years old and even holding a $1,000,000 prize for its completion. This essay aims to explore the fundamental role prime numbers hold as the foundation of encryption, this system's vulnerability and alternatives.

Background theory

Gauss was the father of modular arithmetic, specifically conceptualising his "clock calculator" modelled on the nature of a clock to return to 1 o'clock 4 hours after 9 o'clock, for example. It is when this calculator is used with indices that Fermat's Little Theorem and the star of this essay, the primes, become significant. Fermat's little theorem:

$$a^p \equiv a \,(\mathrm{mod}\, p),$$

where a is an integer and p is a prime number, shows that the remainder when dividing a by p is equal to the remainder when dividing a^p by p, shown by the modular congruence sign (≡).

Euler's totient function $\varphi(n)$ also plays a significant role in encryption. $\varphi(n)$ equals the number of positive integers smaller than and relatively prime to n (HCF is 1). For prime numbers and products of prime numbers, known as semiprimes:

$$\varphi(p) = p - 1$$

$$\varphi(pq) = (p-1)(q-1).$$

Operation of the RSA

The RSA (named after the inventors: Rivest, Shamir and Adleman) chooses two large prime numbers: p and q, over 100 digits long. N is the product of p and q – a semiprime. Positive integers e and d are chosen to satisfy the equation below in order to encrypt and decrypt messages:

$$1 \equiv de(mod\, \varphi(N)).$$

e and N make up the public encryption key used in the encryption formula below, where m is a plaintext message (in binary blocks) and c is the ciphertext encrypted message:

$$c \equiv m^e(mod\, N).$$

The private decryption key is made up of two positive integers: d and N. d is private and kept secret unlike e and N. A message can be decrypted using this formula:

$$m \equiv c^d(mod\, N).$$

The mathematics used by RSA can be proved using Fermat's little theorem.

Example

To illustrate this system of encryption and decryption, consider m (the message) = 3, an easy value to work with albeit worryingly simple for a card number. In addition, let the prime numbers p = 3 and q = 5.

$$m = 3$$
$$p = 3$$
$$q = 5$$

$$N = pq = 3 \times 5 = 15$$

$$\varphi(N) = \varphi(pq) = (p-1)(q-1) = 2 \times 4 = 8$$

$$1 \equiv de(mod\, \varphi(N))$$
$$1 \equiv de(mod\, 8)$$
$$d = 3$$
$$e = 11$$
$$\because 1 \equiv 33(mod\, 8)$$

encryption key $= (e, N) = (11,15)$

decryption key $= (d, N) = (2,15)$

$$c \equiv m^e(mod\, N)$$
$$c \equiv 3^{11}(mod\, 15)$$
$$c \equiv 177147(mod\, 15)$$
$$c = 12$$

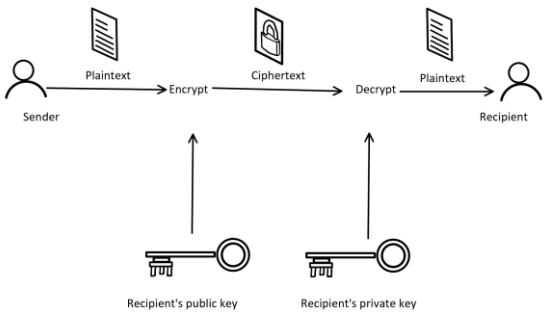
The encrypted message, c, is 12

$$m \equiv c^d(mod\, N)$$
$$m \equiv 12^3(mod\, 15)$$
$$m \equiv 1728(mod\, 15)$$
$$m = 3$$

The decrypted message, m, is 3 which is equal to the original value of m.

Security and factorisation

RSA is a public-key cryptosystem, a type of system that was introduced by W. Diffie and M. Hellman in their paper *New Directions in Cryptography.* This means the encryption key (e, N) is published in a KDC (key distribution centre). Although these details are available publicly, this system is actually significantly more secure than private-key cryptosystems. This is because private-key systems are symmetric, they use the same key to encrypt and decrypt messages. This key has to be exchanged between parties which is very challenging to do securely. On the other hand, it is much more secure for every party to have both a private and public key. The sender can essentially encrypt a message with the recipient's public- key (e, N) so only they are able to decrypt it, using their private-key (d, N). This exchange could be between a web browser and an ecommerce site, for example. Public-key encryption is illustrated in the diagram below:



This characteristic of the RSA means a private-key cannot be eavesdropped, secretly intercepted. However, it is the use of prime numbers which ensures eavesdropped ciphertext cannot be decrypted mathematically without that private-key.

It is computationally infeasible to factorise the product of two very large prime numbers, namely N. Unlike composite numbers with many smaller prime factors that can be found relatively easily, semiprimes like N has only two unique factors. Therefore, when these are particularly large, they are incredibly difficult to find. This leads to the fundamental security of d, for the private-key, as N's prime factors are needed to find it, recall $\varphi((p-1)(q-1)) = \varphi(pq)$ or $\varphi(N)$ for the modulo value. Finding e is described as a "trap-door one-way function," a concept coined by W. Diffie and M. Hellman. This is because it is easy to compute in one direction (e from values p and q) but very difficult in the other direction (p and q from e) due to the difficulty of factorising. To illustrate this difficulty, a challenge was proposed in the *Scientific American* in 1977 for $100. The challenge was to decrypt the ciphertext below, which involves finding the 65-digit and 64-digit primes whose product is used as the modulo value:

9686	9613	7546	2206
1477	1409	2225	4355
8829	0575	9991	1245
7431	9874	6951	2093
0816	2982	2514	5708
3569	3147	6622	8839
8962	8013	3919	9055
1829	9451	5781	5154

A ciphertext challenge worth $100

For interest, the decrypted plaintext turned out to be: "The Magic Words are Squeamish Ossifrage." This took 17 years, a substantial amount of time, although slightly less than the "40 quadrillion years" Rivest estimated in the same article for the factorisation of a 126-digit semiprime.

Quantum computing

Computers have become rapidly more powerful since 1977, when the RSA was first introduced. Therefore the time to factorise using brute force, by exhausting all possibilities, is also rapidly decreasing. The vast computational power of quantum computers also suggests that an attack on the cryptosystem by factorising with brute force is a legitimate concern. The vulnerability of the prime numbers must be questioned.

Quantum computers use quantum bits or qubits which are not just able to represent 0 or 1 but also both simultaneously. In a standard computer, 8 bits, a byte, can represent 256 possible values however using only 8 qubits with a quantum computer all these 256 values can be represented at once.

As technological advancements are made, the time to factorise using quantum computers will become much more reasonable and therefore, threatening to the security of the RSA. However, quantum computing is still a new field of computer science and the resources required to decrypt RSA keys will not be widely available in the imminent future. On the other hand, developments in mathematics, rather than in technology, could pose the most danger to the cryptosystem and businesses that use it.

The Riemann hypothesis

The Riemann hypothesis is a mathematical conjecture about the distribution of prime numbers. A yes or no result about whether the hypothesis is correct will not directly "crack" RSA however it is the mathematics surrounding that proof which could be of interest. This is why technology companies such as AT&T and Hewlett-Packard fund research into prime numbers and the Riemann hypothesis. They want to be the first to know if their security is endangered.

More specifically, research into the mystery of prime numbers may reveal new methods for factorising. The most recent claim to a proof is attributed to Louis de Branges. However, his proofs (of which there have been many attempts) are not widely accepted and Eric Kvaalen in his paper *The application of the de Branges method to prove the Riemann Hypothesis* "found [a recent version] wanting." Acceptance of a proof is essential to the legitimacy of it. For example, the CMI who put up $1,000,000 for each Millennium Problem, including the Riemann hypothesis, specify the importance of acceptance in their rules. A proof must be published for 2 years and rigorously scrutinised by the mathematical community before its author could think about getting their hands on the prize. Therefore, de Branges' claim is unlikely to be taken too seriously and a proof of the hypothesis seems to not be an imminent threat to RSA's security. However, the prospect of future developments in factorisation should not be disregarded and cryptosystems must constantly evolve by investigating new ways of encoding data.

Alternative systems

Rivest, Shamir and Adleman remarked in 1978 that: "the era of electronic mail may soon be upon us". Nearly 50 years later, technology has far surpassed just "electronic mail" to encompass; artificial intelligence, virtual reality, 5G wireless and the aforementioned quantum computing. These advancements illustrate the enormous rise of technology in this period, including the rise of ecommerce and its need for encryption like RSA. The report, *How long can Public key encryption stay secure? Introducing the implications of the Riemann Hypothesis and Quantum Computing,* describes the importance of the security of cryptosystems in ecommerce:

> From individual purchases in an online store, to global inter-bank transactions, our society and all the information underpinning it, is now stored in a digital format interconnected by what has been dubbed the Digital Nervous System. With this digital evolution, any compromise of the current security mechanisms could cause catastrophe on a global scale.

Therefore, to avoid such catastrophe, alternatives must be considered. For example, symmetric private-key systems which are around 1000 times faster than asymmetric public-key ones. They only require one key so are significantly more efficient when it comes to encrypting data. In this type of cryptosystem, a unique private session key can be shared by a trusted KDC (key distribution centre) for each new conversation. However the issue lies with the KDC: if it is corrupted, the entire system is compromised. In addition, a bottleneck can form there as many incoming session key requests pile up to slow down and overwhelm the system, causing it to fail which is significantly disrupting. This is why, for now, public methods of key exchange remain vastly more reliable.

The ultimate cryptosystem would exploits the merits of both private and public methods. This "hybrid" idea was proposed by W. Diffie in his paper *The First Ten Years of Public-Key Cryptography.* Using the current security of public systems to establish keys, involving prime numbers, along with the efficiency of symmetric systems to encrypt. Both parties are able to use the same key to encrypt and decrypt after it is shared in an asymmetric way. Since Diffie's proposal, all currently used public-key cryptosystems have implemented symmetric encryption. Specifically, one session key is distributed between parties asymmetrically to solve issues posed due to a corruption of a KDC. The session key is created when needed and destroyed after use to further decrease risk of compromise in such a short window.

Hybrid systems seem ideal, as long as prime numbers remain secure. The future of cryptography though depends on research into innovative "out-of-the-box" methods beyond the scope of RSA. These could utilise the power and speed of quantum mechanics or alternative verification methods such as biometric data like retinal scans.

Conclusion

The RSA has certainly stood the test of time as one of the first examples of a "trap-door one-way function". Currently, "mathematicians know enough about the primes to build these internet codes, but not enough to break them" (*The Music of the Primes*). The characteristics of prime numbers make them uniquely secure for use in public-key cryptosystems, for now. It would be foolish though to rely on the cryptosystem's longevity as the fundamental difficulty of factorising semiprimes cannot be depended on for much longer. The primary threats that have been considered in this essay include the ever-increasing power of quantum computers to factorise in worryingly short times from the perspective of security. In addition, more research into prime numbers and a proof of the Riemann hypothesis may reveal easier, quicker methods for factorisation besides brute force checking. It is clear that prime numbers are unlikely to be the key to the future of encryption and that methods of encryption in a further 50 years will certainly be unrecognisable to cryptographers of today. Even if the particular threats mentioned do not break the system, there is no doubt that soon there will be discoveries that undermine our dependency on simply not being able to understand the mystery of prime numbers.

Bibliography

Adda, M. Peart, A. McKeever, A. (2005) *How long can Public key encryption stay secure? Introducing the implications of the Riemann Hypothesis and Quantum Computing.*

Diffie, W. (1988) *The First Ten Years of Public-Key Cryptography.*

Diffie, W. Hellman, M. (1976) *New Directions in Cryptography.*

Gardner, M. (1977) *'Mathematical Games,' Scientific American.*

Kvaalen, E. (2016) *The application of the de Branges method to prove the Riemann Hypothesis.*

Rivest, R. Shamir, A. Adleman, L. (1978) *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.*

Sautoy, M. (2004) *The Music of the Primes*.

Schneier, B. (1996) *Applied Cryptography.*