

# Here are my Bank Details:

---

G29kLGrBHLP9aMyTZXzsbb4bx2FExnRIPYkbZ6cHBm6KyGEVJq6Z2vzatgErX/kmWu+ZWQ9RCGm  
Xd0njYpPGqJP3u8iM1608fj64KQgejCfu0RQ4uRuI+rMKnajibQFe0cAHTN2QqFuj7ssiDbUSsXaSjnxY619  
OKeFkV3cJqD6jflwpWrOLK3jF3N3ULsZiHCRmsvZmOpRSv5aSsQUXYDSGpVAI9A55GDytk0MlcaMKb4  
2QQuXdXtNzhdNx9/4i1qj+A9n93a5ljk19t8Mn0VayWg9mehKSZIDx0Qa6RzCr9dbPo/0jFqyXJWTjtmE0  
26CHWOEGxIn/kC+ktzXIA==

## Feel free to take them

That is the main theme of this essay, how information can be kept hidden in plain sight in today's world. The breakthrough of which made e-commerce, banking, secret communications..etc possible and explode on the internet. All thanks to the work of Ron Rivest this along with his colleagues Adi Shamir and Len Adleman.

In this essay I will explore the work and life of Ron Rivest along with my personal opinions of the increasing value of encryption in a world of machine learning lead systems and extremely centralized and controlled computing.

## Ron Rivest

---



## Background

---

Ron Rivest was born in Schenectady, New York on 6th May 1947. Ron grew up and attended public schools in Niskayuna, New York. He went on to study Mathematics at Yale University after graduating from Niskayuna High School in 1965. After completing his B.A. in Mathematics he received a Ph. D in Computer Science from Stanford University in 1974 where his research supervisor was Professor Robert Floyd (of Floyd-Warshall algorithm fame). Not to mention whilst also working closely with the likes of Donald Knuth.

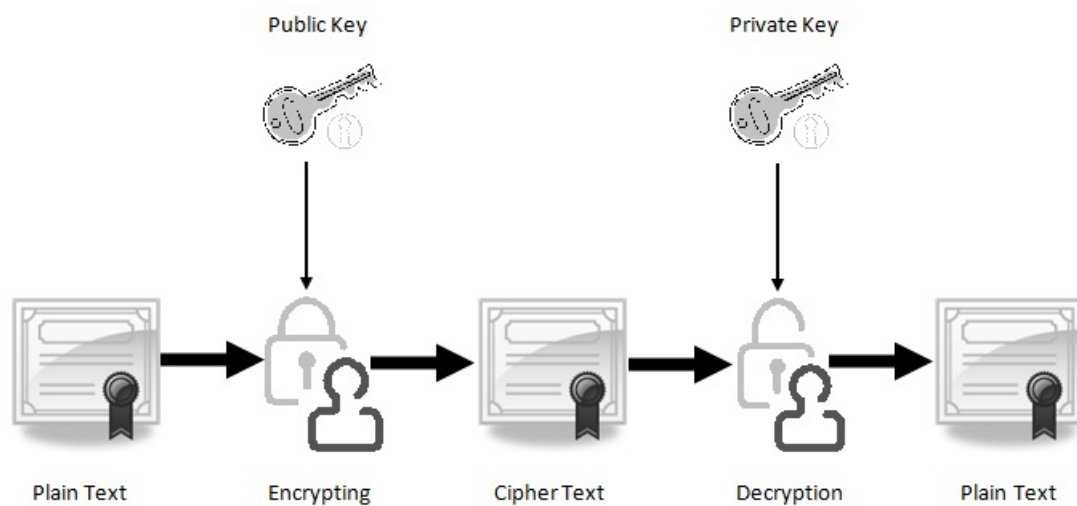
## Key Exchange - RSA

---

At MIT in 1977, Ron worked with Adi Shamir and Len Adleman on a asymmetric key encryption system. It was a response to the open Diffie-hellman problem. The Diffie-Hellman defined a way of doing cryptography called public key cryptography where you could tell someone how to encrypt without telling someone how to decrypt.

It should be noted the the Diffie-Hellman key agreement was first published in 1976 however it wasn't the first time the idea of public key cryptography had been conceptualized. Public key cryptography was shown how it could be achieved by James H. Ellis, Clifford Cocks, and Malcolm J. Williamson of GCHQ in 1969, however this information was held as classified at the time and was only publically released in 1997.

The idea of RSA was that the core difficulty was factoring a enormously large number (consisting of the product of two primes) in order to find the two large prime numbers that give the product of that number. The enormously large number being your public key and the two large prime factors being your private key.



RSA gave the method to allow for posting a public key and allowed for people not be able to figure out information encrypted with that public key however it still has the major difficulty of not knowing how tough/easy it actually is to find the two prime factors of a large number, this can be clearly seen in the RSA-129 example below.

Undoubtedly Ron's involvement helping build RSA is the work he is best known for. He ofcourse puts the 'R' for Rivest in RSA. They also were the first group to use the names 'Bob' and 'Alice' to describe their system, which has since become commonplace in our industry to describe any communication systems. Ron (with A. Shamir and L. Adleman) also won the 2002 ACM Turing Award for their work on RSA.

But his work by no means stopped there...

## RSA-129 - A Tale of Better Algorithms and Moore's Law

RSA-129 = 11438162575788886766923577997614661201021829672124236256256184293  
5706935245733897830597123563958705058989075147599290026879543541

Ron Rivest estimated that it would take about 40 quadrillion years using the current best computing hardware and best algorithms available (in 1977), to solve what the two prime factors were of the above number.

They published an encrypted piece of text with a public key used to encrypt it. The goal was to discover the private key so you can decrypt the text.

If you were able to figure out the two prime factors that make up the above number you could have been in with the chance of winning 100 dollars as they had offered in the Scientified America in 1977.

But sadly this prize has already been claimed by Derek Atkins, Michael Graff, Arjen K. Lenstra and Paul Leyland, using around 1600 computers from around 600 volunteers over the internet in 1994. It was a highly co-ordinated effort over a peroid of around 6 months to solve the problem.

### Answer:

RSA-129 = 3490529510847650949147849619903898133417764638493387843990820577  
× 32769132993266709549961988190834461413177642967992942539798288533

The encrypted text when decrypted stated: "The Magic Words are Squeamish Ossifrage"

What allowed for this to be solved was the massive improvement in computing power but most importantly was the improvement in the algorithms they were using. They used the Multiple Polynomial Quadratic Sieve algorithm which lead to it becoming incredibly more efficient to find the two prime factors.

RSA-129 is a useful reference into the fact that public key cryptography using prime factorisation is not perfect and can be broken however the hopes are that if the individuals select much bigger numbers as the bases for the two prime factors they select, it becomes exponentially harder to crack.

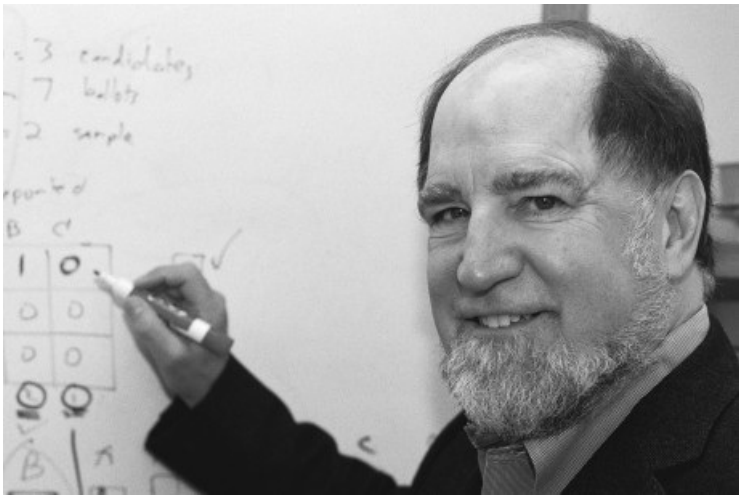
## Work on Symmetric Keys

RSA can be quite intensive and slow to run, due to this, instead of encrypting entire files with RSA encryption, it

is often the case that RSA is used to encrypted symmetric keys, that is a key that can be used to encrypt and decrypt the same file. By encrypting a symmetric key with RSA, you can decrypt your symmetric and then use someone elses' public RSA key in order to encrypt the symmetric key for them.

Allowing for your files to be encrypted with the symmetric key, the symmetric key being encrypted via RSA, allowing for the one version of encrypted files to be shared among as many as you want, simply by encrypting another symmetric key.

Ron also worked on symmetric key cryptography too. With symmetric key encryption algorithms such as RC2, RC4, RC5, and helped co-invent RC6, the RC standing for 'Ron's Code' originally. However as Ron states on his site "RC6 was co-developed with Matt Robshaw, Ray Sidney, and Yiqun Yin of RSA Labs, so it is only "Ron's code" in part..."



## Hashing - MD4, MD5, MD6

Along with his work on asymmetric and symmetric key encryption Ron also worked on various extremely popular cryptographic hashing algorithms. Hashing isn't meant to be an encryption, it is a "message digest" algorithm. Which means the original input is not meant to be easily recoverable that isn't the goal. Usually you just want to test does X input when put through MD5 give the same output you have previously stored.

This was an extremely popular method of storing passwords, due to improvement of algorithms and computing hardware however it has since been severely undermined and is seen as bad practice to store passwords with in the modern day, especially when there is no use of salting in the password input.

Ron had authored the cryptographic hash functions: MD2, MD4, MD5 and MD6.

Now if you google an MD5 hash you are often able to see the original input that lead to that MD5 hash output. But at the time it was a major breakthrough for password security.


## Voting

Ron also has an interest in voting systems, he published the ThreeBallot system in 2006. Which he put into the public domain as according to him "Our democracy is too important". The main point of the ThreeBallot system was that a voter could discern their vote that was counted whilst protecting their privacy.

BALLOT		BALLOT		BALLOT	
President		President		President	
Alex Jones	<input type="radio"/>	Alex Jones	<input type="radio"/>	Alex Jones	<input type="radio"/>
Bob Smith	<input type="radio"/>	Bob Smith	<input type="radio"/>	Bob Smith	<input type="radio"/>
Carol Wu	<input type="radio"/>	Carol Wu	<input type="radio"/>	Carol Wu	<input type="radio"/>
Senator		Senator		Senator	
Dave Yip	<input type="radio"/>	Dave Yip	<input type="radio"/>	Dave Yip	<input type="radio"/>
Ed Zinn	<input type="radio"/>	Ed Zinn	<input type="radio"/>	Ed Zinn	<input type="radio"/>
3147524		7523416		5530219	

Essentially they would be given three ballots, each with an identifiable number. On two of the ballots they made to make them cancel out. E.G. In an election between Bob and Alice. And the voter wanted Alice to win. So in two of the ballots they would mark Alice with an X then in the other ballot they would mark Bob with an X. So that overall Alice got 1+ vote in comparsion to Bob. This meant that if ballots go missing, it would be easier for a voter to detect this. There has been some criticism of this system as people argue it isn't very usable.

## Educational Influence



Rivest co-authored "Introduction to Algorithms" with Charles E. Leiserson, Thomas H. Cormen and Clifford Stein. A staple of any Computer Science degree. It was first published in 1990 and between then and 2010, it had sold over half a million copies. What makes it unique is that no answer guide given. Along with his written work he is currently an Institute Professor at MIT. And has also featured in other educational content online such as the youtube channel "Numberphile" created by Brady Haran.

## Why Ron Rivest Inspires me

Ron has without a shadow of a doubt been hugely influential in Algorithms, Cryptography and Voting. His work immensely propelled the industry forward. I personally believe cryptography and voting mechanisms are more important than ever. I believe in a future in which there is much more decentralized systems (decentralized NOT being ICOs or cryptocurrency alone), but protocols such as the dat protocol where it is much more similiar to torrents but for websites.

I believe this type of completely decrentalized system is necessary for the future but it could only be possible if sensitive information can be encrypted with symmetric keys and public key prime factorisation encryption used to encrypt the symmetric key for multiple people to use. I am fascinated of the idea of everyone having the information but the encryption is so strong it doesn't matter, only those with the correct private keys can make sense of it. That is why Ron Rivest inspires me as a programmer.

## Sources Used

- Ron Rivest - Numberphile Playlist: <https://www.youtube.com/watch?v=YQw124CtvO0&list=PLt5AfwLFPxWJN-idOLqOJNdAPBN9zahTa>
- Ron's MIT site: <http://people.csail.mit.edu/rivest/>
- AM Turning Award - Rob Rivest Bio: [https://amturing.acm.org/award\\_winners/rivest\\_1403005.cfm](https://amturing.acm.org/award_winners/rivest_1403005.cfm)

***The encrypted paragraph does not contain actual bank details...but it makes a great opener...***

**Here are the Public and Private Keys, for those of you who like a little adventure:**

-----BEGIN PUBLIC KEY-----

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAinNzRqKbnsgJksWw8rgRjUmUVmeyisLFnY1KMvG72tw3C77C0DpVmH4KDAeUhdxoieb2VUBO/oBhWB5TOtK+kyF3l0Kb5+uFQeDeQ6EFWfI9IA9UDF/fR9yYiuBLLh/AL0chUCIpdmE+13oCMC4U2tLx0zimLg5Ge216se/xyUIRefBe31Bj76xajZ7qKOyo8wDlvEdYVj9L11wpE6WN9Ly8kjeVSd5ApGM+2nQ4x2NTjK9Bj5WXVSs9WJGAYqYQFDpEiTZOG8YJmwKhKe6qH+W4AK+xd01Ze2fdTOtCwLYjZWGuxU9+kjd2gPvMz6kO9+aiZr0VcT0DzyauDQQWnwIDAQAB
```

-----END PUBLIC KEY-----

-----BEGIN RSA PRIVATE KEY-----

```
MIIEpAIBAAKCAQEAinNzRqKbnsgJksWw8rgRjUmUVmeyisLFnY1KMvG72tw3C77C0DpVmH4KDAeUhdxoieb2VUBO/oBhWB5TOtK+kyF3l0Kb5+uFQeDeQ6EFWfI9IA9UDF/fR9yYiuBLLh/AL0chUCIpdmE+13oCMC4U2tLx0zimLg5Ge216se/xyUIRefBe31Bj76xajZ7qKOyo8wDlvEdYVj9L11wpE6WN9Ly8kjeVSd5ApGM+2nQ4x2NTjK9Bj5WXVSs9WJGAYqYQFDpEiTZOG8YJmwKhKe6qH+W4AK+xd01Ze2fdTOtCwLYjZWGuXU9+kjd2gPvMz6kO9+aiZr0VcT0DzyauDQQWnwIDAQABAoIBAApMeje34tGHyqeDUx1K+9KjPYiL4CkYQfDtUKaneqzWERyp833fyPw16/NnIPlwKgqQBqTiyR19uT//yXsnsAtrwuSajNRcnaX/3yiysp41w8v9t+fPveEvIj1H/+ +nZvldVioK0IDAzRbkOYNx+hUo+doXba0hXLBtTvvDeH3bfU0lmd+Rtys58Hm93JXqF3Nr3+lihvmFMXyB
```

7lexgFNiQJU2wmMWbFRicxDsFF2OIRcYil/ZONxK1EM5yFb0qXf3NSKUSQU3K/tH  
AN9w4nxww9QHGCGRVYjbL0ADvB6DkXeYEQG+iXeJuY1nPVKsS8iYzluPQ8Pzncqy  
wq6tIMkCgYEAvRe31FOZtTyQwE7UmUOhhrkeV7F9JUdXfQnThPmxY+Jiw6A6x3WB  
ARgMzjLxvRE2oZXG1MzLuMstYpxGy76i1iVjFqRmsCG3ADT1yiKYzmyjhGqqMwoj  
ebqexb0lLkB0GyQVgP4Lg5m23alCWyhFoysJO6X9hI8pgNnyrRumCb0CgYEAu3CJ  
ksgFGQqJNfn0yByNzkifvbXNEZrIVuEZx81LEnJraJAjXpAbiGTBLMnK/QRshEw1  
X8UpuHCyXUeNrqr/KRiNf51si+LWhcclq66nahkRWbihqJzDyjZ7QzB2uedAgqdo  
MGn5Zquqf14CtrZ6w+whw/8yLzKp0RSTqXxoUYsCgYEAnF4nu2Kiwjfib9UAg/lk  
cpdU2ynAFnrHg3QDwXwGUFYeXC19TglCexgbRszkEPHSGA9WjBULBralwlz/Qm9U  
Ewh5x3iOHmrS/U3OT6iKenFmSxM1yd0r9sj3kQeX3oaYPPV6/t+WP+52RRk58U39  
QDBPg08BtYP5yz7wKmypwnUCgYEAuB57hOtI1os67QJzKH6j7RX5k+iZX8m/re+/  
dRO7wosSZsvvclwsL3ajKu2tr4xA7FPPuht6N+q7ylUXH5RowH2VwN1qWp6gCxjs  
MBCH8vhcyr1KTs5upJuPyRg6B7LY835uleB3VBSch7BZChGF1h6FrHlpWmNx3CdS  
RRInhrECgYAUZa2GtepETI8q7SzzFPHkMch2KKaA/Zpib6tLjyx2HhyQ2NRqg+8L  
0G1he2TTdylhof6ibkSKiAlJ7gLLiWYSb8ip2gWcYcH7F63YO4y7gufMx2nDSw6R  
P3AdrW6/ru6jFErHMAVZu72b2bnHPXRrQuN1apQWMm3DlabdlzJ4Cg==

-----END RSA PRIVATE KEY-----