How Secure is RSA: Mathematical Approach

By: Rana Khalil, Undergraduate
Supervisor: Dr. Monica Nevins, Professor and Chair
University of Ottawa, Faculty of Science

Introduction

Cryptography is the art and science of writing in secret code. With the advent of the Computer Age, cryptography has become essential in today's economy. Public key cryptography is based on mathematical problems that currently admit to no efficient solution. This in turn has allowed individuals to share secret communication over insecure channels, such as the internet, which begs the question: **How secure are public key algorithms?** Recently, it was revealed that the National Security Agency (NSA) has obtained access to RSA protected information by exploiting some unknown flaws. In this research we analyze a paper by Lenstra et al. called "Ron was wrong, Whit is right" which identifies some of these potential flaws. Our project is to understand the mathematical theory behind two major algorithms: RSA and Diffie Hellman, with the probability of these flaws occurring.

Prime Numbers

There are infinitely many prime numbers which are randomly distributed. The prime number theorem states that for a randomly chosen number N, the probability that it is prime is 1/ ln (N), i.e. prime numbers are “easy” to find.

X	2	3	4	5	6	7	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

Table 1. Sieve of Eratosthenes from 1 to 100

Discrete Logarithm Problem

Let g and h ∈ **Z**/p**Z**. The Discrete Logarithm Problem (DLP) is the problem of finding an exponent x such that $g^x \equiv h \pmod p$
The number x exists if g is a primitive root for **Z**/p**Z**.

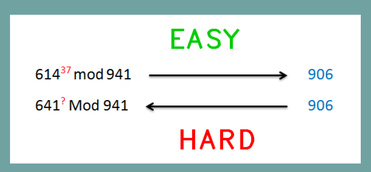

Figure 1. DLP example

Note: Exponentiation mod p is random; see Chart 1 for an example with p=941.

Methods and Materials

(I) Symmetric Cryptography

Symmetric encryption algorithms work on one basic principle- the same key that is used to encrypt the plaintext is used to decrypt the ciphertext.

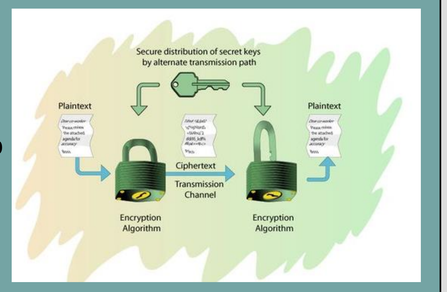

Figure 2. Symmetric Key Cryptography

Public Parameter Creation	
A trusted party chooses and publishes a (large) prime p and an integer g (which is a primitive root for Z/pZ) having large prime order in **Z**/p**Z***.	
Private Computations	
Alice	**Bob**
Choose a secret integer a. Compute $A \equiv g^a \pmod p$.	Choose a secret integer b. Compute $B \equiv g^b \pmod p$.
Public Exchange of Values	
Alice sends A to Bob →	A
B	← Bob sends B to Alice
Further Private Computations	
Alice	**Bob**
Compute the number $B^a \pmod p$.	Compute the number $A^b \pmod p$.
The shared secret key value is $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod p$.	

Table 2. Diffie-Hellman key exchange

(II) Asymmetric Cryptography

Asymmetric encryption and decryption uses separate keys. Decryption is done using the private (secret) key, while encryption is done using the public key.

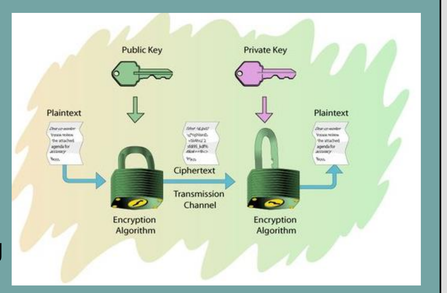

Figure 3. Asymmetric Key Cryptography

Alice	**Bob**
Key Creation	
Choose secret primes p and q. Choose encryption exponent e with gcd(e, (p – 1)(q – 1)) = 1 Publish N (= pq) and e.	
Encryption	
	Choose plaintext m. Use Alice's public key (N, e) to compute $c \equiv m^e \pmod N$ Send ciphertext c to Bob.
Decryption	
Compute d satisfying ed ≡ 1 (mod (p – 1)(q -1)). Compute $m' \equiv c^d \pmod N$. Then m' equals the plaintext m.	

Table 3. RSA key creation, encryption, and decryption

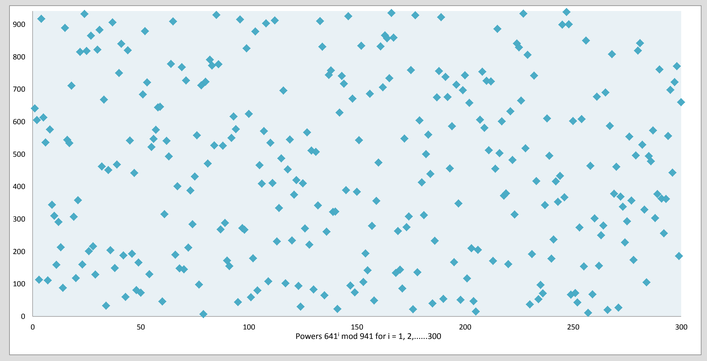

Chart 1. Distributions of discrete logarithms for g = 641 modulo p = 941

Symmetric	RSA, DL	Comments
64 Bit	70 Bit	Short term security
80 Bit	1024 Bit	Medium security
256 Bit	3072 Bit	High security

Table 4. Key lengths and Security Levels

Results

Flaw: In the Lenstra et al. paper it was mentioned that among 4.7 million 1024-bit RSA moduli collected, more than 12500 have a single prime factor in common! This flaw allows for easy factorization of n.
Analysis: By the prime number theorem, there are approximately 2^{504} primes that are less than 2^{510}. Therefore, the odds that two people randomly choose at least one prime factor in common is

$$P = 1 - \left(\frac{2^{504}-2}{2^{504}}\right)^2 = 1 - \left(1 - \frac{1}{2^{503}}\right)^2 \approx \frac{1}{2^{502}}$$

However, if we sample M (= 4.7 million) different N, then the odds that two of these N’s share at least one common factor is approximately,

$$1 - (1 - P)^{\frac{M(M-1)}{2}} \approx \frac{M(M-1)}{2} P \approx \frac{2^{43}}{2^{502}} \approx \frac{1}{2^{459}} \approx 0$$

Conclusion

In conclusion, the mathematics behind RSA is still very solid. The major flaw detected by Lenstra et al. seems to be an implementation error not a mathematical error. For further research refer to [2], [3] & [4].

First and foremost, I would like to thank God for giving me the opportunity to participate in this research. I would also like to thank UROP for providing me with the funding and resources to complete my research. Lastly, special thanks to Dr. Monica Nevins for taking time out of her very busy schedule to teach me about the fascinating world of cryptography!

109417386415705274218097073220403576120037329454492059909138421314763499842889347847179972578912673324976257528997818337970765372440271467435315933543338 97

Rana Khalil
University of Ottawa, Undergraduate Research Opportunity Program (UROP)
rkhal101@uottawa.ca

References:
1. Hoffstein, J. , Pipher, J. , Silverman, J. H. , (2008). *An Introduction to Mathematical Cryptography.* New York, NY: Springer Science+Business Media.
2. Mironov, I. (2012, May 15) . Factoring RSA Moduli. Part I. . Retrieved from windowsontheory.org/2012/05/15/979/
3. Mironov, I. (2012, May 17) . Factoring RSA Moduli. Part II. . Retrieved from windowsontheory.org/2012/05/17/factoring-rsa-moduli-part-ii/
4. Lenstra, A. K., Hughes J. P., Augier, M., Bos, J. W., Kleinjung T. & Wacher, C. (2012). *Ron was wrong, Whit is right, 064*. Retrieved from eprint.iacr.org/2012/064.pdf
5. Survivability and Information Assurance (n.d.). Retrieved March 16, 2014, from http://people.ubuntu.com/~duanedesign/SurvivabilityandInformationAssuranceCurriculum/02everything/02everything.html#AEN379