Public Key Cryptography Timeline (With focus on the RSA System)

1969 According to the Government Communications Headquarters (GCHQ) in Cheltenham. James Ellis had ideas about public key cryptography that Diffie and Hellman later published. However, because Ellis was sword to secrecy by the British Government, he could not publish his findings. He also figured out that he needed one way functions that could be reversed if a receiver had some sort of special information.

1976 Whitfield Diffie and Martin Hellman published a paper entitled "New Directions in Cryptography." They suggested a system that used keys that were publicly know and could be authenticated by use of powers and one-way functions. However, they did not provide a specific application of their system.

1973 Clifford Cocks, also working for the GCHQ, developed the same system Rivest, Shamir, and Adleman discovered four years later. His discovery was also kept secret because of his oath to the British Government.

1977 Ronald Rivest, Adi Shamir, and Leonard Adleman figured out how to make a public key system. This system was practical because it included digital signatures and was based on the difficulty of factoring large primes. The system's security is based on the usage of large primes (hundreds of digits) to prevent factoring algorithms from working.

1977 Martin Gardner said it would take millions of years (with 1977 computer speeds) to decode a message encoded in RSA-129. It was projected that by deciphering the message, it would require factoring a 454-digit number and would be a milestone in cryptography. He offered a $100 reward for breaking the system. It was broken in 6 months time in 1994.

1978 The RSA System was published in the *Communications of the ACM*, a widely-known technical magazine.

1994 Martin Gardner's challenge was met and the RSA-129 system was broken. This shows that if a problem in 1977 would take millions of years, and only 6 months in 1994, technology is improving more rapidly than expected. In other words, the key size and modulus are weakened with the advancement in technology.

Timeline Sources

Atkins, Derek. Georgia Institute of Technology. 02 May 2003. <http://www.security.gatech.edu/protection/rsa/rsa129challenge.html>.

Churchhouse, Robert. Codes and Ciphers: Julius Caesar, the Enigma, and the Internet. New York: Cambridge, 2002.

Ellison, Carl. Cryptography Timeline. 16 April 2003. <http://world.std.com/~cme/html/timeline.html>.

Singh, Simon. The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography. New York: Doubleday, 1999.