Project Bibliography

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

This site gives information about Martain Gardner's challenge to break the RSA system and describes how it was broken in 1994.

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

This book gives historical background information on public key cryptography. It also describes the Diffie-Hellman key exchange and RSA systems in explicit mathematical detail. This book compliments the Applications of Abstract Algebra with Maple text very well by providing a different explanation for encryption and decryption techniques.

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

Ellison gives a timeline that contain information on public key cryptography. The public key cryptography part is very short, but gives a rough outline.

Kahn, David. The Codebreakers: The Story of Secret Writing. New York: Scribner, 1996.

This book describes how pubic key cryptography came about. It provides no mathematical background, but excellent historical information.

Klima, Richard, Neil Sigmon, and Ernest Stitzinger. Applications of Abstract Algebra with Maple. New York: CRC, 1999.

This book sparked my interest in public key cryptography and provides the most complete mathematical explanation of all the sources I found.

Schneider, Fred. Public Key Cryptography. 16 April 2003 <http://www.cs.cornell.edu/Courses/cs513/2000sp/L26.html>.

This website graphically describes the problems with public key cryptography and how the Diffie-Hellman key exchange works. This site will be useful in presenting the algorithm from a different standpoint.

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

This book provides information on how the RSA System was born from the Diffie-Hellman key exchange paper. It describes the history in detail and talks about each key person involved (Diffie, Hellman, Rivest, Shamir, and Adleman). It also describes a controversial issue of who discovered public key cryptography and the RSA system first.