

Twenty years after receiving it as a Christmas present, I have finally got around to reading *The Code Book* by Simon Singh. Written in 1999, when E-commerce was still relatively new, the book provides accessible explanations of the workings of Diffe-Hellman-Merkle key exchange, and Rivest, Shamir and Adleman (RSA) public-key cryptography.