Clayton Cohn

Prof. John Rogers

CSC 440 - 810

16 Mar 2019

Final Exam

Short Answer. For the short answer portion of the exam, I chose the Twofish cryptosystem. At its core, the Twofish cryptosystem is a symmetric block cipher. It has a block size of 128 bits, and takes a key of any length up to 256 bits (NIST required all competing algorithms to accept 128, 192, and 256-bit keys) (Schneier 3). It outputs 128 bits of ciphertext—the same size as the plaintext block. Twofish is a Feistel network. Each round includes half of the block being sent through some function, the result of which is XORed with the other half of the block (Schneier 4).

The Twofish encryption algorithm is as follows. First, we start with our 128-bit block of plaintext, and our (up to) 256-bit key. The key generates 40 subkeys via a key schedule. 8 of the subkeys will be used in the "whitening" (XORing) process—4 right after the initial plaintext input, and 4 right before the ciphertext output. The other 32 keys will be used during the cipher's 16 rounds—2 per round. The plaintext is initially separated into 4 32-bit "words," and each word is whitened with one of the subkeys before the rounds begin (as mentioned above). Because Twofish is a Feistel network, there is a left side and a right side. The two left-most words make up the left side, and the two right-most words make up the right side. One of the two left words is rotated left 8 bits, then each left word is used as an input to the g function. The g function consists of four 8-bit S-boxes, followed by a "linear mixing step" based on the MDS (Maximum Distance Separable) matrix (Aparna IV). Afterwards, the two results of the g functions are combined via PHT (Pseudo-Hadamard Transform), and the two subkeys for that round are added (mod 2^32). On the right side, one of the words is rotated left 1 bit, and then both of the right-side words are XORed with the results from the left. The right-side word that did not previously rotate then rotates to the right 1 bit. At this point, the right side becomes the next round's left side, and the original left side becomes the next round's right side. There are 16 rounds in all. After the final round, all four words go through one more round of whitening with the remaining four subkeys, after which all four words are concatenated, and final ciphertext returned.

Confusion occurs in the cryptosystem during the whitening process, where the key is split into subkeys, and those subkeys are XORed with the text block before the first round and also after the last round. The S-boxes also create confusion, as S-box selection is key-dependent. The Twofish key schedule was specifically designed to, "prevent related-key attacks and to provide good key mixing" (Schneier 12).

Diffusion occurs in the mixing via the MDS matrix, which was chosen specifically to "provide good diffusion" (Schneier 10). Also, the PHT, along with the key addition, "provide diffusion between the subblocks and the key" (Schneier 11). The various bit shifts also aid in diffusion.

The cipher's nonlinearity is derived from the S-boxes. Like many block ciphers, Twofish utilizes S-boxes as a "non-linear fixed substitution operation" (bdimciu 6). The S-box operation cannot be put into a linear equation, making the cipher nonlinear.

The Twofish cipher was designed by: Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. Bruce Schneier is considered to be the primary designer (Wikipedia Twofish). He is a "cryptographer, computer security professional, privacy specialist and writer" (Wikipedia Bruce Schneier). He is from Brooklyn, New York, and is currently a fellow at the Berkman Center for Internet & Society at Harvard Law School. He received a bachelor's degree in physics from the University of Rochester, followed by a Master's in Computer Science from American University, and was later awarded an honorary PhD from the University of Westminster. He has worked for Harvard University, Counterplane Internet Security, Bell Labs, U.S. Department of Defense, and BT Group (Wikipedia Bruce Schneier).

Works Cited (short answer)

bdimciu. “Twofish Encryption Algorithm on ZYBO.” *Instructables*, Instructables, 19 Sept. 2017, www.instructables.com/id/Twofish-Encryption-Algorithm-on-ZYBO/.

K, Aparna, et al. “A Study of Twofish Algorithm.” *IJEDR*, Volume 4, Issue 2, 2016, www.ijedr.org/papers/IJEDR1602023.pdf.

Schneier, Bruce. “The Twofish Encryption Algorithm.” *Schneier on Security*, 1998, www.schneier.com/academic/archives/1998/12/the\_twofish\_encrypti.html.

Wikipedia Contributors. “Bruce Schneier.” *Wikipedia*, Wikimedia Foundation, 13 Mar. 2020, en.wikipedia.org/wiki/Bruce\_Schneier.

Wikipedia Contributors. “Twofish.” *Wikipedia*, Wikimedia Foundation, 6 Oct. 2019, en.wikipedia.org/wiki/Twofish.