Jackson Warren

Jeremy Bergen

CSCI 370

10/6/21

Week 10 Assignment

As a general description: cryptographic algorithm is the process of altering data from a plaintext and readable format to one that is in a protected form, or ciphertext, and finally back again. One such example of these cryptographic algorithms is called Triple Data Encryption Algorithm (TDEA).

1. TDEA is a block stream cipher, with 64-bit block sizes. This is noticeably smaller than current standards, being 128-bit minimum for most current ones, since collisions can occur every 2^32 blocks. Also, to aid in protections, TDEA has a blended key length of 168 bits, as it is three 56-bit keys.
2. Part B:
   * 1. Explicitly designed for Encryption: TDEA is not a great algorithm, and has vulnerabilities. It was ranked “medium”, and is only actually secure for about 112 bits, rather than the full 168. Both brute force and meet-in-the-middle attacks pose it vulnerable. Its block size was also small, as mentioned before, so not great. So although I didn’t find anything knocking its encryption techniques, it lacked in overall strength with its techniques.
     2. Security Not Dependent on Secrecy: With TDEA being outdated and no longer used really, its security measures are fully available. So, I don’t believe this still matters for the algorithm since it is now outdated and no longer secure.
     3. Available for analysis: Now, once again, the algorithm is open for analysis but is simply shut down. During its analysis, it was susceptible to several attacks where it had weak points. Having the meet-in-the-middle weakness due to the multiple encryption keys was analyzed and found weak, as well as the brute force attacks, breaking in with 2^56 space and 2^112 operations.
     4. Subjected to analysis: As stated just above, it was no doubt subjected to this analysis and came up lacking, hence the reason it was replaced with AES largely.
     5. No Practical Weaknesses: Well, I think this section is pretty evident by my previous answers. It is practically weak and did not protect what it needed to well enough. Once again, the reason it is not recommended.
     6. Cryptographic Evaluation: Alright, I searched for a while for this and could not find anything on TDEA doing this test. I believe many of the current standards for this test were in fact a result of the weaknesses TDEA had. I also believe that TDEA would’ve failed the test so they didn’t exactly boast about it.

References:

Aslam, S. (2020). *Comparison Of TDEA And Rijndael Advance Encryption Standard (AES)*. Comparison Of TDEA And Rijndael Advance Encryption Standard (AES). https://www.c-sharpcorner.com/article/comparison-of-tdea-and-rijndael-advance-encryption-standardaes/

*Cipher-or-cryptographic-algorithm Meaning | Best 1 Definitions of Cipher-or-cryptographic-algorithm*. (1997). YourDictionary. https://www.yourdictionary.com/cipher-or-cryptographic-algorithm

Turner, D. M. (2019). *Summary of cryptographic algorithms - according to NIST*. Summary of Cryptographic Algorithms - According to NIST. https://www.cryptomathic.com/news-events/blog/summary-of-cryptographic-algorithms-according-to-nist