Compatibility and choice for symmetric key decision-making for block ciphers

Part 1:

Team Name: Hostage Situation

Names:

Alvin Crighton
Rohin Dasari
Brandon Vo

For our project, we decided to opt for project 2 type 2 where we would design a Q&A system such that it would inquire and guide a fresh user as to what ideal cryptographic scheme he/she would like to use. Our decision tree would function based on the cryptographic primitive of block ciphers and symmetric encryption schemes.

Part 2:

- A second deadline (TBD) requires you to go to Quizzes and submit the design of your method/solution, in any desired form, so to obtain instructor/TA feedback before starting implementation (the instructor will not go over too many details of your design but will tell you if he can quickly see any major design flaws or omissions or improvement opportunities). You can later change the design as well.

For our implementation, we decided on using a classification tree to decide what general method of encryption the user might want. The implementation will be using scikit's decision tree machine learning package where feedback will be obtained based on user responses.

Because this decision tree would be designed for the symmetric block cipher cryptographic primitive, extensive research was done on 5 unique block cipher schemes that had different design goals and intentions to achieve secrecy and correctness. The set was also chosen due to being recognized as a secure scheme and proven to have not been declared broken within reasonable probability.

AES-128

- State-modified
- Operates for 10 rounds.
- Every step in AES is fast and efficient due to its simplicity
- Requires only one encryption and decryption key

- Perfect secrecy and encryption achieved through permutation and diffusion (changing one byte will drastically change the output)
- Non-linear and high diffusion
- Cyclic
- While no practical attacks have been discovered, AES is mentioned as having simplicity and efficiency prioritized over complex but secure methods.
    - Has noticeable differential patterns
    - The best attack that can be done still takes 2^190 operations (when using 7 rounds).

- **Triple DES**
    - Was widely adopted and implemented in its legacy years
        - Still used in legacy software over AES in certain cases
    - Very slow compared to the rest of the cryptography schemes
    - Limited to 56 bit key lengths and 64 bit block size
    - Operates for 48 rounds.
    - Will be officially deprecated by 2023 by NIST
        - Broken due to the discovery of the Sweet32 birthday attack

- **IDEA**
    - Patent free as of 2012, meaning everyone is free to use this algorithm (Still needs to get licensing approval from the creator).
    - Widely supported for open source projects
    - Operates for 8.5 rounds
    - Smaller memory requirements compared to AES but uses more complex operations
    - Was considered fast and efficient at the time, but has been overtaken by modern cryptographic schemes.
    - Vulnerable only if used for 6 rounds or less. Otherwise, requires atleast 2^128 procedures to break
    - Has weak keys which leads to weak encryption procedures
- **SIMON**
    - Relatively new, being made in 2013 by the NSA
        - Controversial regarding whether or not this algorithm is actually safe because of this reason.
    - Operates for 44 rounds (Using a 128 key size)
    - Was officially supported on Linux kernels as of Feb. 2018.
    - Designed for lightweight computers with severely limited resources
    - Focused on maintaining an acceptable level of security for extremely low-end hardware.
        - SIMON was mainly designed for low-end hardware. Its sister scheme, Speck, was designed for software.
- **Threefish-1024**
    - Based off the Skein hash function and Twofish encryption scheme

- Uses alternating additions with XORs as part of its encryption schemes to achieve nonlinearity
- Keysize is variable going up to 1024-bits.
- Encryption process runs for up to 80 rounds depending on the key length.
- Despite the large block size and large number of rounds, Skein is mentioned to be designed to be faster than SHA-512 if the implementation was tweaked to be optimized for speed.
- While Threefish has been implemented in devices that can't even run AES, Threefish, in general, is harder to find from a cryptographic library and is extremely specialized, making it more difficult to find support for compared to AES.
- Threefish-1024 sacrifices additional memory for better security and collision resistance.

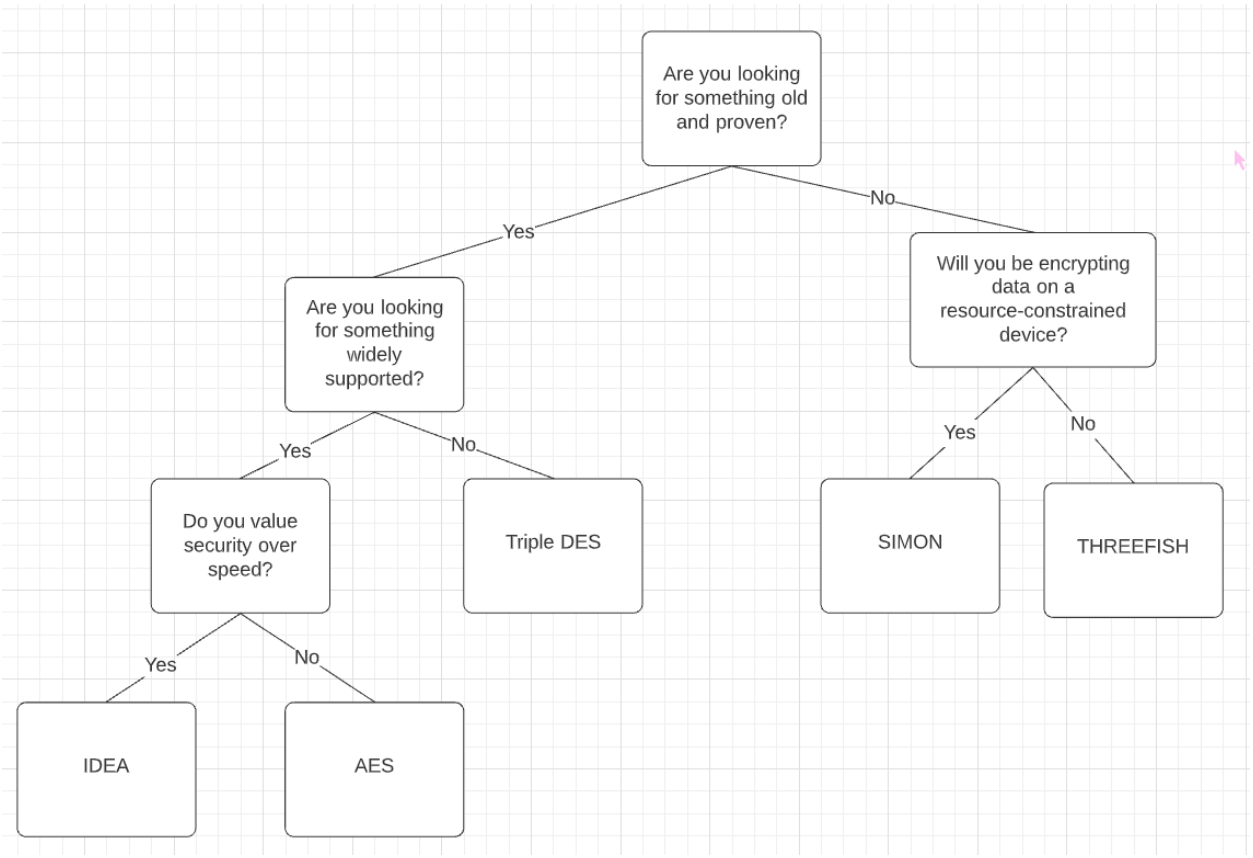
While some schemes may have different results based on various factors such as hardware and implementation designs, the attributes given to the cryptographic schemes were assigned based on design intent rather than empirical data as benchmarking tests have variable results based on what hardware is being used. For example, SIMON was declared to be faster and more efficient on AES for specifically low-end hardware that is unable to run AES efficiently, but SIMON's implementation paper describes the design intent for SIMON to be a cryptographic scheme that can maintain a baseline level of security for low-end hardware. This reasoning means that SIMON was designed for security over speed.

Number of operations to crack	**Runtime (clock cycles per byte)**	**Block Size (Bits)**	**Old and proven or new and unknown?**	**Widely supported?**	**Complex or Simple**	**Output**
2^{113}	108	64	Old (1975)	Until 2023	Simple	Triple DES
infeasible	18	18	Old (1998)	Yes	Simple	AES-128
$2^{125.7}$	7.5	Flexible	New (2013)	Yes	Simple	SIMON
$2^{126.1}$	132	64	Old (1991)	Yes	Complex	IDEA
2^{222}	881	1024	New (2008)	No	Complex	Threefish-1024

Using information from the constructed table, the questions were designed based on the contrasting attributes found amongst the five block cipher schemes. In order to understand what the user does or does not want, the questions were designed based on what the user is willing to sacrifice in return for a secure cryptographic scheme.

For example, a developer for an instant-messaging service would prioritize sending messages as soon as possible and might be more willing to use smaller, faster cipher schemes to achieve that goal whereas a developer for an e-mail messaging client might not be as concerned with sending an email on time and would be more willing to sacrifice extra time for a more rigorous encryption method.

As a result, the questions that would be asked by our decision tree would approximate the user's desired scheme from asking what attributes would be more preferable for the user and what properties of a block cipher that the user is willing to give up. This reasoning led us to create the following decision tree outline.



Sources:

AES encryption method and properties:

https://ro.uow.edu.au/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1176&context=theses

AES vs. IDEA

https://www.sciencedirect.com/science/article/pii/S0026269208005661#:~:text=The%20AES%20implementation,implement%2016%20SBox%20by%20phase.

José M. Granado, Miguel A. Vega-Rodríguez, Juan M. Sánchez-Pérez, Juan A. Gómez-Pulido,
IDEA and AES, two cryptographic algorithms implemented using partial and dynamic reconfiguration,
Microelectronics Journal,
Volume 40, Issue 6,
2009,
Pages 1032-1040,
ISSN 0026-2692,
https://doi.org/10.1016/j.mejo.2008.11.044.
(https://www.sciencedirect.com/science/article/pii/S0026269208005661)

SIMON resources:

https://github.com/nsacyber/simon-speck

Linux announcing support for SPECK and SIMON

https://www.mail-archive.com/linux-crypto@vger.kernel.org/msg30853.html

IDEA on the cryptowiki:

https://www.cryptopp.com/wiki/IDEA

AES vs. SIMON

https://csrc.nist.gov/csrc/media/events/lightweight-cryptography-workshop-2015/documents/papers/session1-shors-paper.pdf

https://www.mail-archive.com/linux-crypto@vger.kernel.org/msg30853.html

Triple DES vs. AES

https://symbiosisonlinepublishing.com/computer-science-technology/computerscience-information-technology32.php

https://www.baeldung.com/cs/des-vs-3des-vs-blowfish-vs-aes

Triple DES Sweet-32 attack

https://sweet32.info/

IDEA encryption attack

Biham, E., Dunkelman, O., Keller, N. *et al.* New Attacks on IDEA with at Least 6 Rounds. *J Cryptol* 28, 209–239 (2015). https://doi.org/10.1007/s00145-013-9162-9

Co-author of Threefish discusses Threefish's security:

https://crypto.stackexchange.com/questions/11725/has-threefish-successfully-been-attacked-practically-or-theoretically

Comprehensive comparison of symmetric block cipher schemes:

http://paper.ijcsns.org/07_book/201812/20181218.pdf

https://eprint.iacr.org/2010/538.pdf

http://article.nadiapub.com/IJSIA/vol9_no4/27.pdf

Threefish's implementation issues:

https://crypto.stackexchange.com/questions/42463/what-encryption-should-i-use-blowfish-twofish-or-threefish

Skein-1024 vs. Skein 256 (Threefish's algorithm):

https://crypto.stackexchange.com/questions/16029/skein-state-size-advantages

Skein implementation benchmarking

https://www.schneier.com/wp-content/uploads/2015/01/skein.pdf

Importance of Block Size for Encryption:

https://crypto.stackexchange.com/questions/35450/how-does-blocksize-affect-security

NIST report on Block Ciphers:

https://csrc.nist.gov/CSRC/media/Publications/sp/800-131a/rev-2/draft/documents/sp800-131Ar2-draft.pdf

Alternative block ciphers:

- https://en.wikipedia.org/wiki/IDEA_NXT
- https://en.wikipedia.org/wiki/Serpent_(cipher)