Phillip Kimbrel

In the situation for the best algorithm cipher I would have Artemis financial use would have to be AES (Advance Encryption Standard). The reason for this as this will encrypt everything from the CPU to storage and files. This will make sure that there will be multiple keys that will have to be decrypted to get into the data as we can everything from passwords to files and disks the data is on. With AES we can run the encryption and decryption on almost anything, making it the best to use even on a budget. If you don’t use modern CPUs you might be opening yourself up to side-channel attacks as modern hardware has AES encryption and more cores making it harder to do. Known-key distinguishing attacks could be used to try and get in to the files and see the plaintext but they would have to get through The disc and partition encryption first. This is the best cipher as most of the attacks proposed on it are mostly theoretical and trying to brute force it would take forever. The way AES works it that each block cipher in 128 bits and are put into a 4x4 grid array each point having 16 bits and the key size can be one of three different sizes for 128, 192, or 256 bits . The keys length determines the amount of rounds of encryption the input will go through. Each round goes through 4 steps Sub bytes where each byte gets substituted with another; shift rows where the rows of bits are shifted a certain number of times; then mix columns in which this step uses multiplication by multiplying each column with a matrix changing each byte in the column; and then the final step is adding a round key

**References**

GeeksforGeeks. (2024, July 16). *Advanced Encryption Standard (AES)*. GeeksforGeeks. https://www.geeksforgeeks.org/advanced-encryption-standard-aes/

Mowery, K., Keelveedhi, S., & Shacham, H. (n.d.). *Are AES x86 Cache Timing Attacks Still Feasible?* Retrieved June 8, 2025, from http://cseweb.ucsd.edu/~kmowery/papers/aes-cache-timing.pdf