اسم الطالب: عبد الله محمد جاسم

Cryptographic Hardware: Design of AES and RSA accelerators

Size	The report does not specify the number of personnel, but notes an increase in physical "Chip Area." Designing custom hardware (ASICs/FPGAs) requires a highly specialized engineering team, indicating a complex and non-trivial project size.
Cost	**High.** The report explicitly states under "Trade-offs" that manufacturing dedicated hardware accelerators is more expensive compared to pure software-only solutions.
Purpose	To **improve the technical infrastructure** and operations. The primary goal is to solve the processing bottlenecks and high power consumption of standard CPUs, providing high-speed, secure data processing for servers, mobile devices, and autonomous vehicles.
Length	Not explicitly stated in the report. However, designing, testing, and manufacturing custom cryptographic hardware inherently takes significantly more time before value is delivered compared to developing software updates.
Risk	1- Short-term risks involve the high upfront manufacturing costs and increased silicon space. A major long-term risk mentioned is the future threat of quantum computers, which requires the project to design "flexible" accelerators ready for Post-Quantum Cryptography (PQC).
Scope	Likely the **entire corporation**, or at least the entire IT and Cybersecurity division. Implementing hardware-level encryption changes the foundational infrastructure for how all organizational data and communications are secured.
Return on investment (ROI)	ROI is measured in massive performance and efficiency gains rather than immediate cash revenue. The report highlights an **encryption speed increase of 10x to 100x** (1000% to 10000%) and an **energy consumption reduction of up to 80%**, leading to massive long-term savings on operational and power costs.