COMPUTER security plays an important role in securing our most important strategic resources – the information. One of the best ways to secure the computer systems is through cryptography. Cryptography focuses mainly on issues of ensuring the information confidentiality, integrity, authentication and non-repudiation. From the security point of view, cryptographic algorithms are expected to deliver the highest level of security services for computer systems. At the same time, these algorithms must be efficient in term of performance to comply with the intensive and sensitive transactions. Currently, there are numerous cryptographic algorithms being used to provide computer systems with various security services. Unfortunately, the structures of these cryptographic algorithms are found sequential in term of their data processing mechanisms, while parallel processing with multi-core technology is becoming more of a common practice. Therefore, there is a clear gap between the implementation of sequential cryptographic algorithms and the future of multi-core processors; the current cryptographic algorithms are not prepared to embrace the enhancement brought by the multi-core processors. This talk proposes few possible alternatives to bridge the gap between the powerful multi-core processors and the sequential structures of current cryptography. These alternatives are designed with a focus on optimum utilization of the multi-core processors. It is expected that by exploring the proposed alternatives, new essential findings will be identified to benefit the development of future parallel cryptography.