

In this paper, we present the hybrid cryptographic scheme and its application in safeguarding the dissemination of both public and commercial data in static state or in transaction, which also expedites faster computational processes. The application is derivable from the asymmetric and symmetric hybrid encryption schemes. The asymmetric schemes are number-theoretic operations which are slower than the symmetric encryption schemes that always uses block enciphers. Often, it is the desire in most encryption schemes to encrypt long messages, but with the asymmetric key only; this could pose time depletion due to its slowness in process execution. To achieve accelerated coding preeminence, it is always appropriate to use the two well-known encryptions paradigms-the Public Key Infrastructure (PKI) and the Private Key Infrastructure (Secret Key). In practice, an encoder will first encrypt her private key using the recipient's public key, and then sends her encrypted key embedded in her encrypted message that is encrypted with her public key. The recipient upon receiving the contents of the message will decrypt the transmitted encrypted key using his private key since this was encrypted with his public key; then with the decrypted private key from the sender, he decrypts the message of the sender since the sender uses her public key to encipher the message. This process is called hybrid encryption scheme. Our proposal is to scrutinize the functionality of this encryption scheme and then apply it on our discourse of Cyberspace terrorism warfare for national security top secret advantage. We present an ingenious algorithmic cryptosystem based on encryption and decryption Oracles for the construct.