Number theoretical foundations in cryptography

ABSTRACT

In recent times the hazards in relationships among entities in different establishments worldwide have generated exciting developments in cryptography. Central to this is the theory of numbers. This area of mathematics provides very rich source of fundamental materials for constructing secret codes. Some number theoretical concepts that have been very actively used in designing crypto systems will be highlighted in this presentation. This paper will begin with introduction to basic number theoretical concepts which for many years have been thought to have no practical applications. This will include several theoretical assertions that were discovered much earlier in the historical development of number theory. This will be followed by discussion on the ñhiddenò properties of these assertions that were later exploited by designers of cryptosystems in their quest for developing secret codes. This paper also highlights some earlier and existing cryptosystems and the role played by number theoretical concepts in their constructions. The role played by cryptanalysts in detecting weaknesses in the systems developed by cryptographers concludes this presentation.

Keyword: Cryptography; Number theoretical