# Cryptanalytic Methods on Block Cipher: Application to GOST Cipher

Wun-She Yap
Centre for Cyber Security
Universiti Tunku Abdul Rahman

**Abstract**

Symmetric key cryptographic primitives are frequently employed in existing security applications for communication purposes due to their superior efficiency in terms of speed as compared to public key cryptographic primitives. Out of all symmetric key cryptographic primitives, the block cipher is the most widely used symmetric key primitive in real-life applications as the block cipher can be used as the core component in building other symmetric key primitives such as the stream cipher, hash function, message authentication code and modes of operation. It is important for the third party to perform additional security analysis on the security of block ciphers as such analysis serves as the certificate of its security strength and the pitfalls that designers should be mindful of when designing a block cipher. In this talk, we first provide the background that is needed to understand the construction of a block cipher and describe the resources needed to quantify a cryptanalytic attack. Subsequently, we present some commonly used cryptanalytic methods to attack block ciphers. Finally, we demonstate how an attacker can apply such cryptanalytic methods on GOST cipher which is a Soviet and Russian government standard symmetric key block cipher.