

# Glossary

- **AES** Advanced Encryption Standard.
- **DES** Data Encryption Standard.
- **IBM** International Business Machine.
- **NBS** National Bureau of Standards.
- **NIST** The National Institute of Standards and Technology.
- **FIPS** Federal Information Processing Standard.
- **RC6** Rivest Cypher 6.
- **NSA** National Security Agency.
- **RSA** Rivest, Shamir, Adleman.
- **QKD** Quantum Key Distribution.
- **ITS** Information Theoretic Secure.
- **ECB** Electronic Code Book.
- **CBC** Cipher Block Chain.
- **CFB** Cipher FeedBack.
- **OFB** Output FeedBack.
- **CTR** Counter.
- **COA** Ciphertext only attacks.
- **KPA** Known plaintext attacks.
- **CPA** Chosen plaintext attacks.
- **CCA** Chosen ciphertext attacks.
- **MITMA** Man-in-the-middle attacks.
- **XOR** Exclusive OR Function.
- **GF** Galois Field.
- **HLES** High Light weight Encryption Standard.
- **WPF** Windows Presentation Foundation.
- **GUI** Graphical User Interface.