

Symmetric Cryptography Protocols

Thierry Sans

Security goals vs attacker's model



Let us consider **confidentiality, integrity and availability**