

COMP3441/9441 Tutorial Week 10

Symmetric Ciphers

1. What is the birthday paradox? Why is it important to cryptography?
2. Why are symmetric ciphers not always appropriate for digital signatures?
3. How do Substitution-Permutation networks work? Give some examples of SP-network ciphers.
4. How do Feistel ciphers work? Give some examples of Feistel ciphers.
5. What is *avalanche*?
6. What is *key scheduling*?