Lecture 6

Stream and Block Ciphers

Stream Ciphers  
convert plaintext to ciphertext one bit at a time under a different key. Eventually the key will repeat. Faster and easier to implement. Examples are Vigenere, Beaufort, and rotor ciphers

Block Ciphers  
  
Confusion – hiding individual characters in the

Diffusion – ensuring that one character in the plaintext affects all other characters; unique to block ciphers

1. a
   1. RFID can store a far wider variety of information that a barcode, and data can be recognised at a much higher temperature (95% at 70 > 99.9% at 120)
   2. Embedded type tags were used in the first development. They need to consider weight, wear, adhesiveness, heat, pressure and cost.
   3. Between development stages, they changed the type of tags used