Symmetric Encryption

Thierry Sans

Design principles (reminder)

1. **Kerkoff Principle**
   The security of a cryptosystem must not rely on keeping the algorithm secret

2. **Diffusion**
   Mixing-up symbols

3. **Confusion**
   Replacing a symbol with another

4. **Randomization**
   Repeated encryptions of the same text are different