Some desirable properties for any cryptosystem

Recall Kerckhoff's Principle: A cryptosystem should be secure when the attacker knows all the details of the encryption and decryption algorithms but does not know the secret key.

i.e. No security through obscurity of the method

Definition: A cryptosystem is *unconditionally secure* if it cannot be broken, even with infinite computational resources.

Additional desirable properties for block ciphers

- **Confusion:** The relationship between the key and cipher text is obscured.

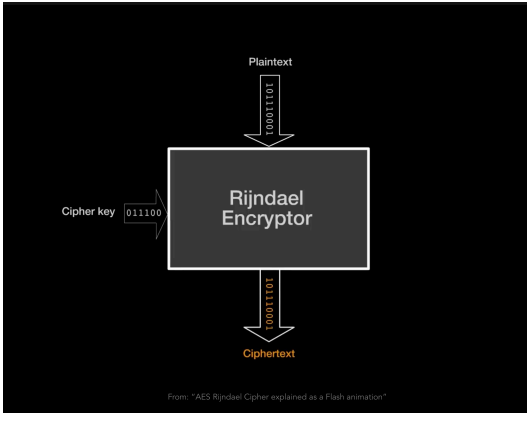
  i.e. Each bit of cipher text should depend on several parts of the key so that if one bit of the key is changed, then the cipher text should appear to be changed randomly.

- **Diffusion:** Each plaintext symbol affects many parts of the cipher text.

  i.e. If one bit of plain text is changed, then much of the cipher text is changed.

Rijndael / Advanced Encryption Standard

- Symmetric block cipher with 128/192/256 bit key
- Open knowledge how all components determined
- Much of remainder of semester looking at how Alice & Bob exchange keys



General structure of AES

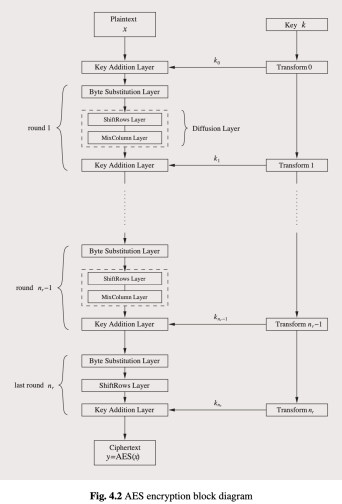


Fig. 4.2 AES encryption block diagram

From Paar, Pelzl, and Güneysu

1. Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$
   (a) Find the following in $\mathbb{Z}_4$, if they exist: 1^{-1}, 2^{-1}, and 3^{-1}
   (b) How many elements of $\mathbb{Z}_4$ have a multiplicative inverse?

2. Repeat #1 for $\mathbb{Z}_5$.
   That is, for each non-zero $a \in \mathbb{Z}_5$, find a^{-1} if it exists, and count the number of elements of $\mathbb{Z}_5$ that have a multiplicative inverse.

3. Repeat #1 for $\mathbb{Z}_7$, $\mathbb{Z}_8$, and $\mathbb{Z}_{15}$

4. Ponder your answers. What patterns or relationships do you notice?