Stream ciphers vs. Block Ciphers

Convert plaintext to bits $x_0, x_1, \ldots, x_b$

- Stream cipher encrypts one-bit at a time

- Block cipher encrypts entire block at once

  Algorithm may use all bits to create ciphertext

  Will see a version of AES that uses 128-bit blocks

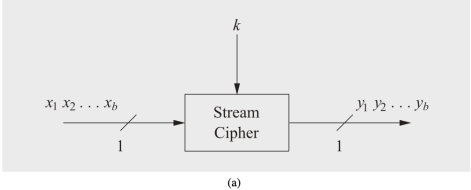

Fig. 2.2 Principles of encrypting b bits with a stream (a) and a block (b) cipher

From Paar and Pelzl, pg. 30

The goal is to encrypt the word “Pi?” using a stream cipher

1. Look up the Unicode 16.0 encoding for “P”, “i”, and “?” at `https://unicode.org/charts/` (*Look under the Basic Latin script*)

2. Convert each encoding to a binary number and combine to get a 48 bit value This is the plaintext x

3. Encrypt x using the key stream:

$$s = 1010\ 1010\ 1010\ 1010\ 1010\ 1010\ 1010\ 1010\ 1010\ 1010\ 1010\ 1010$$

   Note this is a silly key stream, but makes the computation tractable by hand