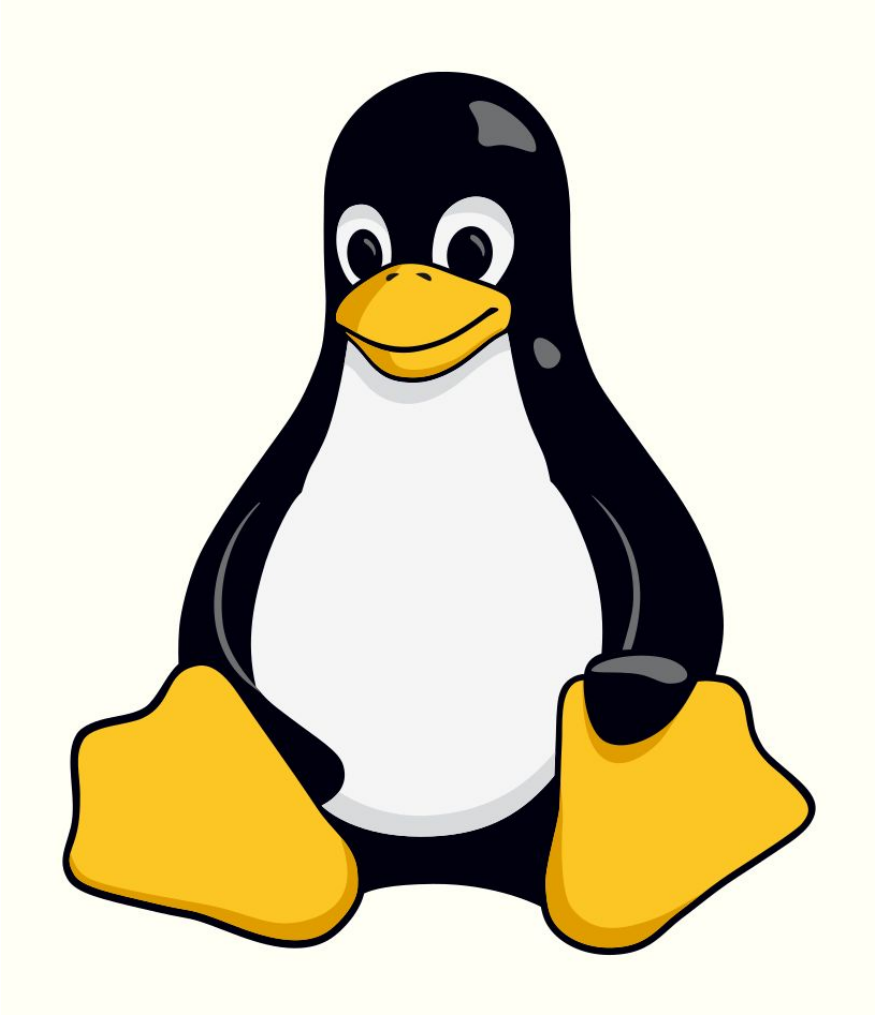
Encrypting the penguin

“Hands-on theoretical workshop”

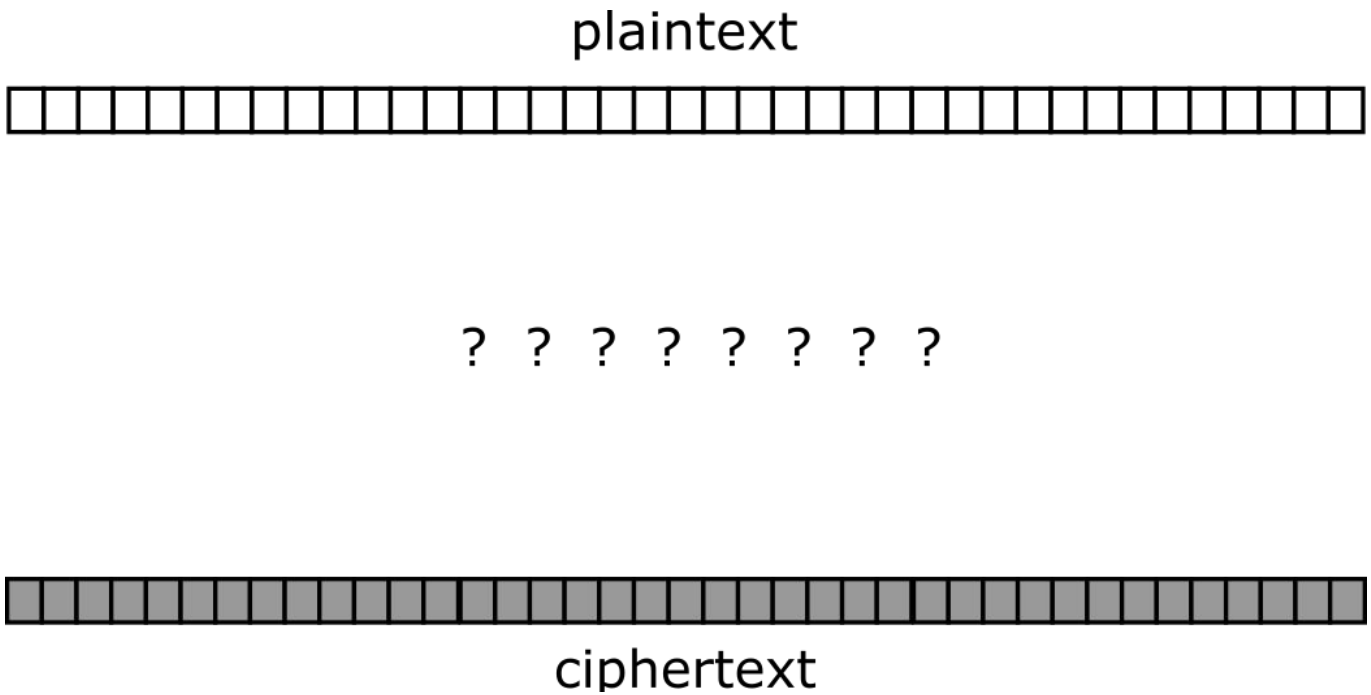
Designed by Martin Ukrop
mukrop@mail.muni.cz
Masaryk University, Czech Republic

TACK
COMPUTER SCIENCE TEACHING ACTIVITIES

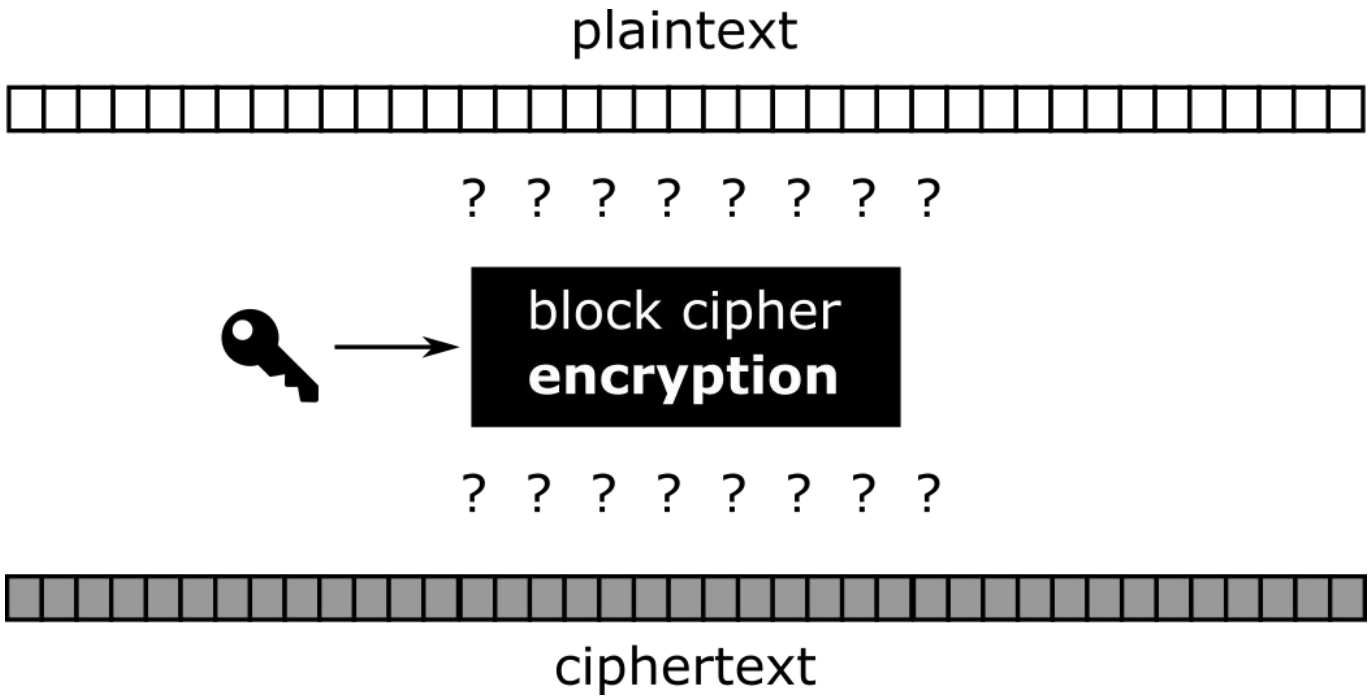
Need for encryption...



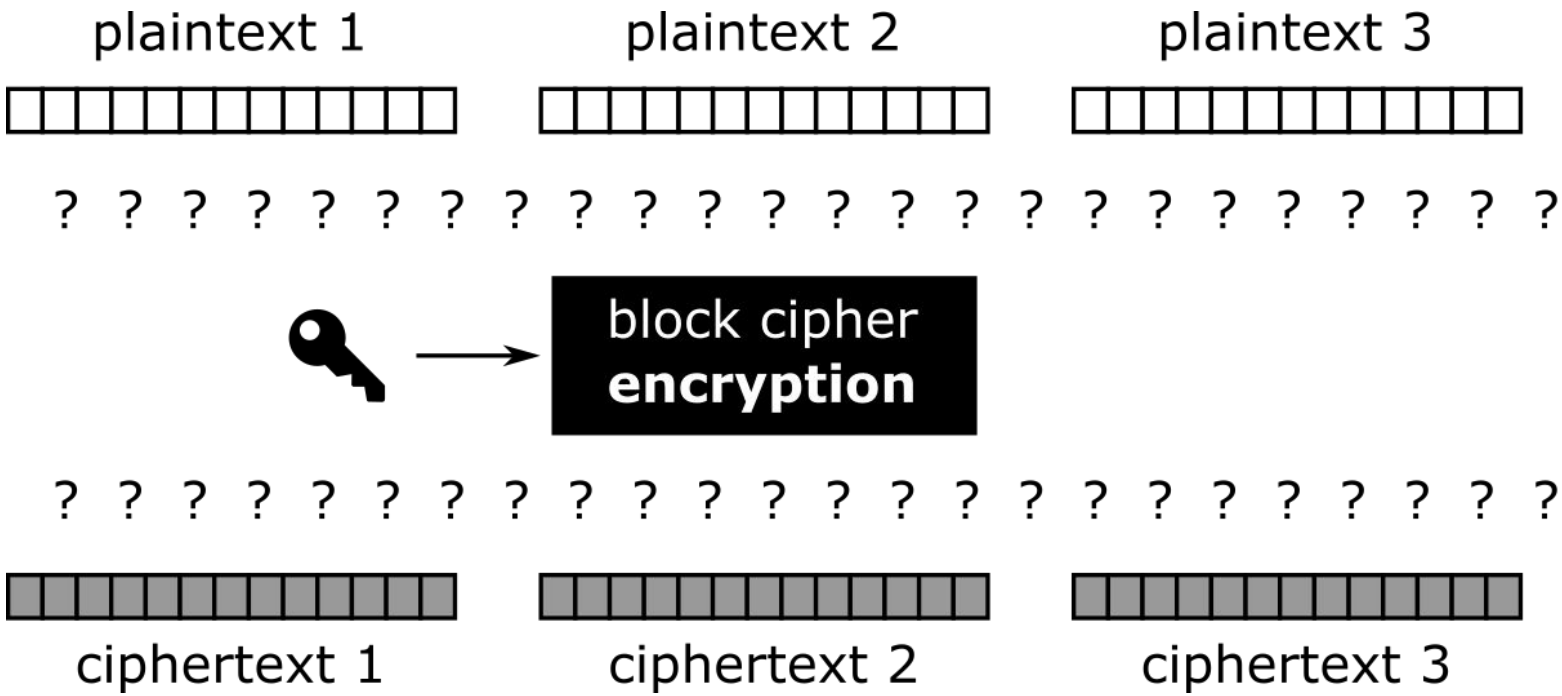
Need for encryption (in the abstract)



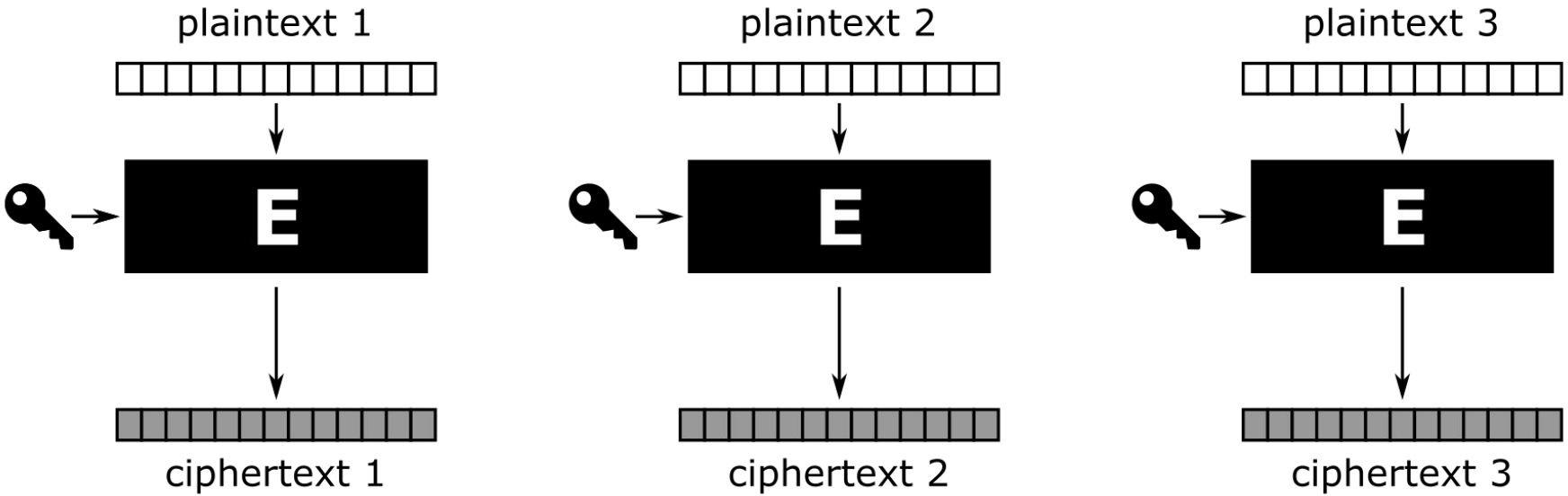
Block cipher to help!



Cutting plaintext in small, workable pieces

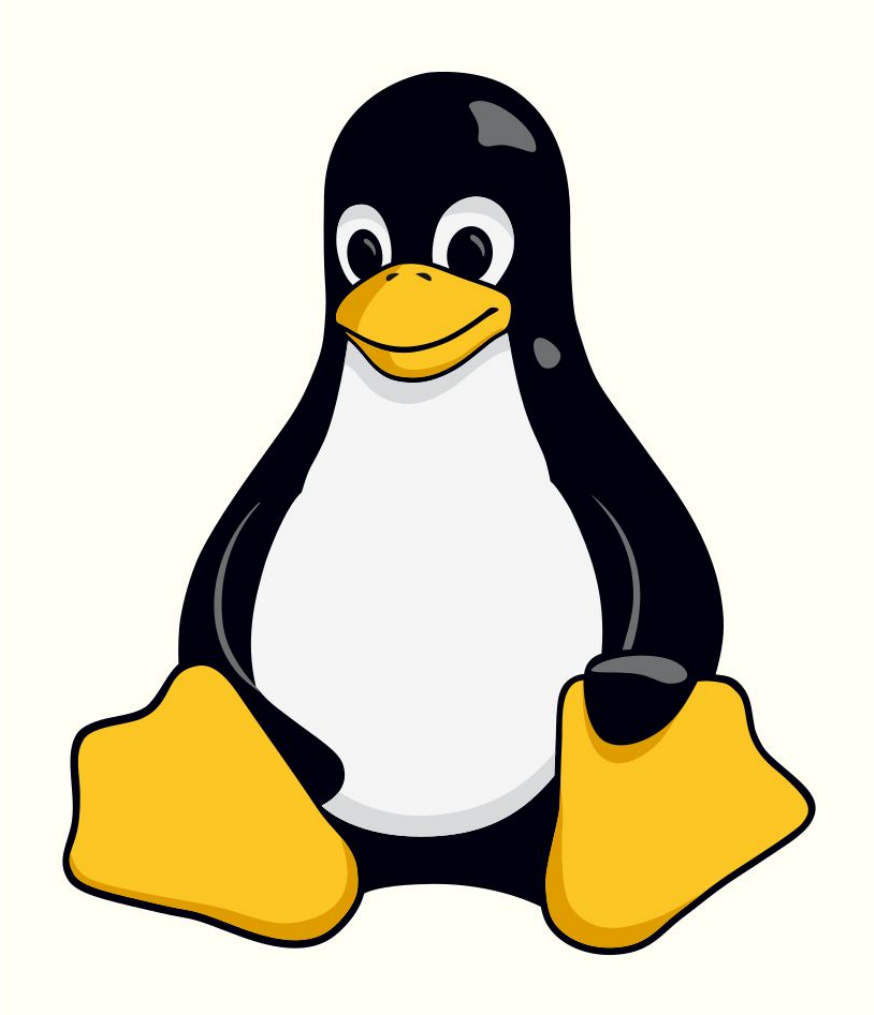


Electronic code book (ECB)



Encrypting TUX

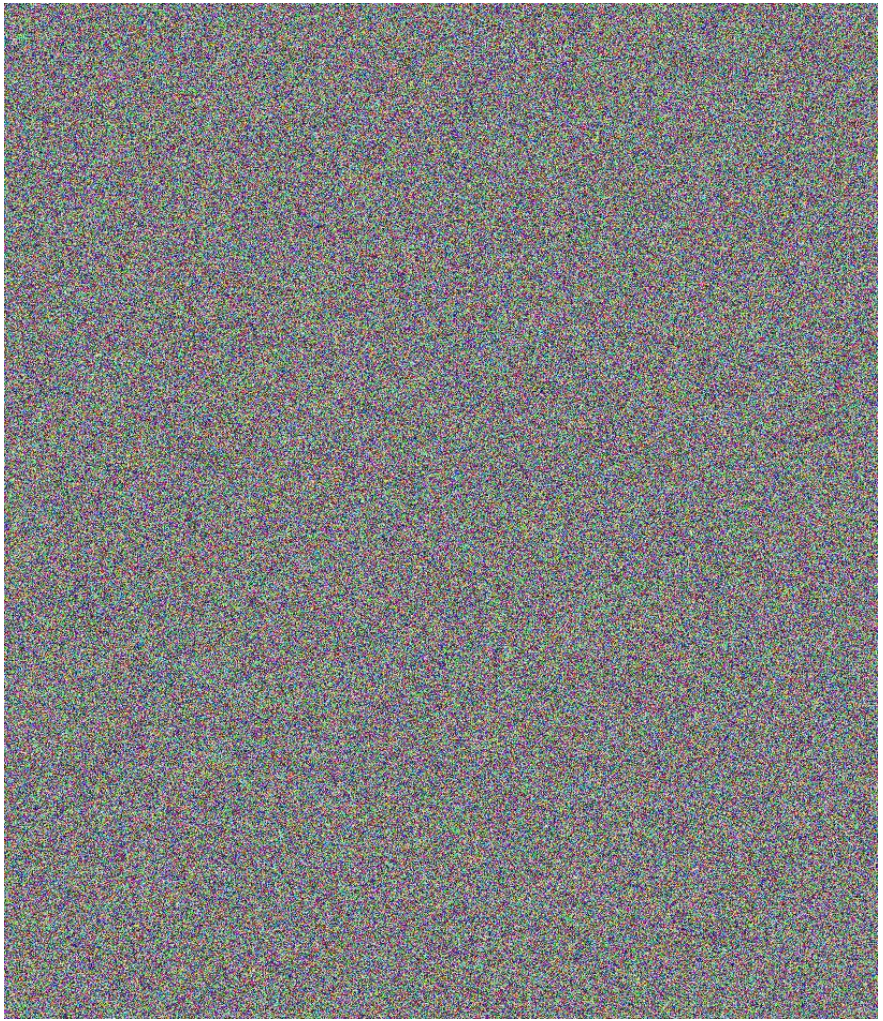
(plaintext)



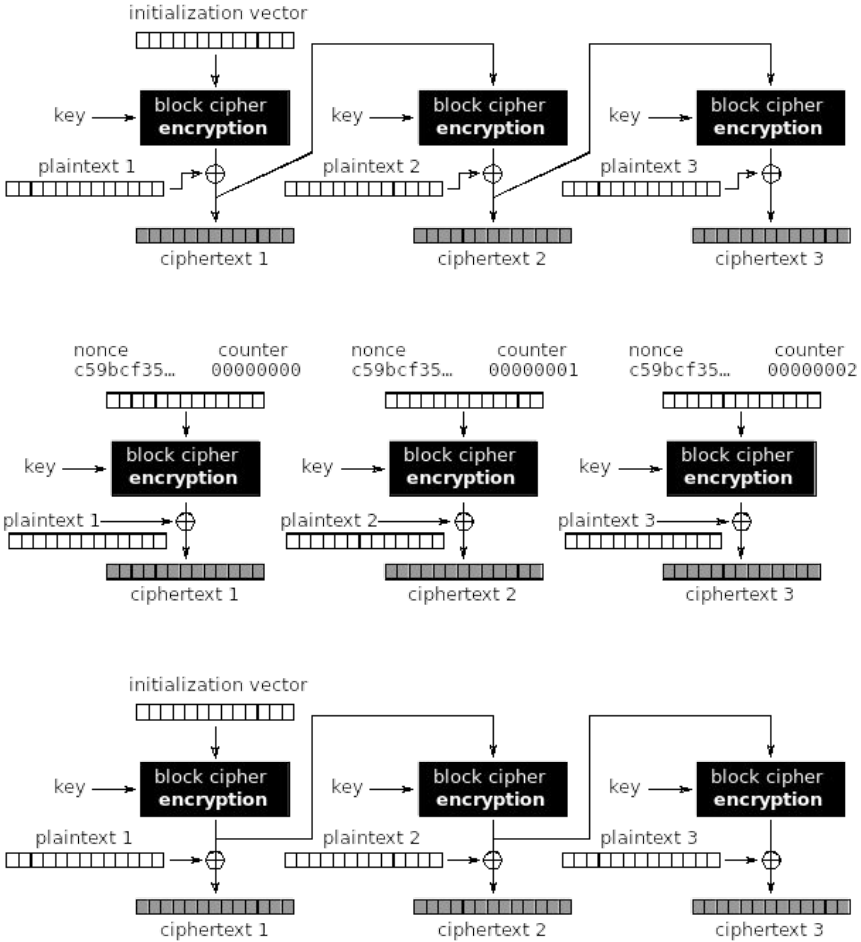
Encrypting TUX

(ECB ciphertext)

We can do much better!



We can do much better!



Features of XOR (eXclusive OR)

1. Binary exclusive operation for simple “encryption”

$$\begin{array}{r} 0\ 0\ 1\ 1 \\ \oplus\ 0\ 1\ 0\ 1 \\ \hline 0\ 1\ 1\ 0 \end{array}$$

2. XORing with the same string “decrypts” the original

$$\begin{array}{r} 0\ 1\ 1\ 0 \\ \oplus\ 0\ 1\ 0\ 1 \\ \hline 0\ 0\ 1\ 1 \end{array}$$