Encryption modes

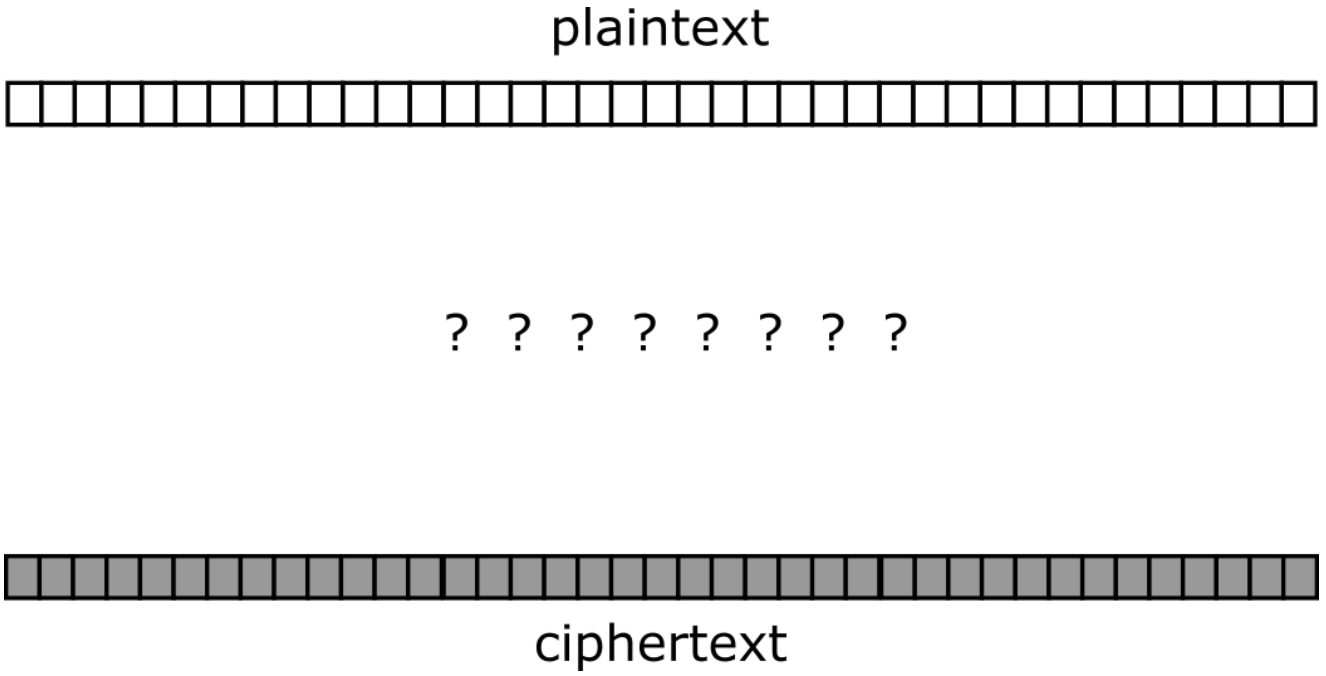
“Hands-on theoretical workshop”

Martin Ukrop mukrop@mail.muni.cz
Faculty of Informatics, Masaryk University

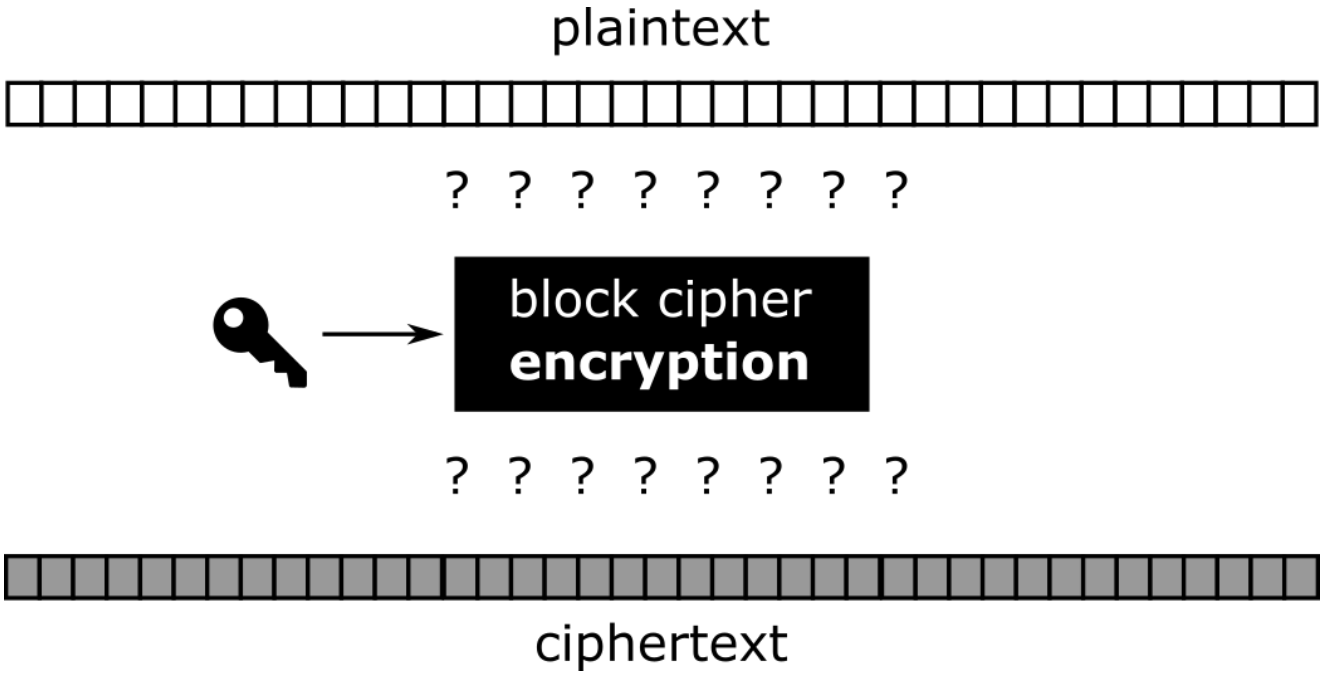
CROCS
Centre for Research on Cryptography and Security

Need for encryption...

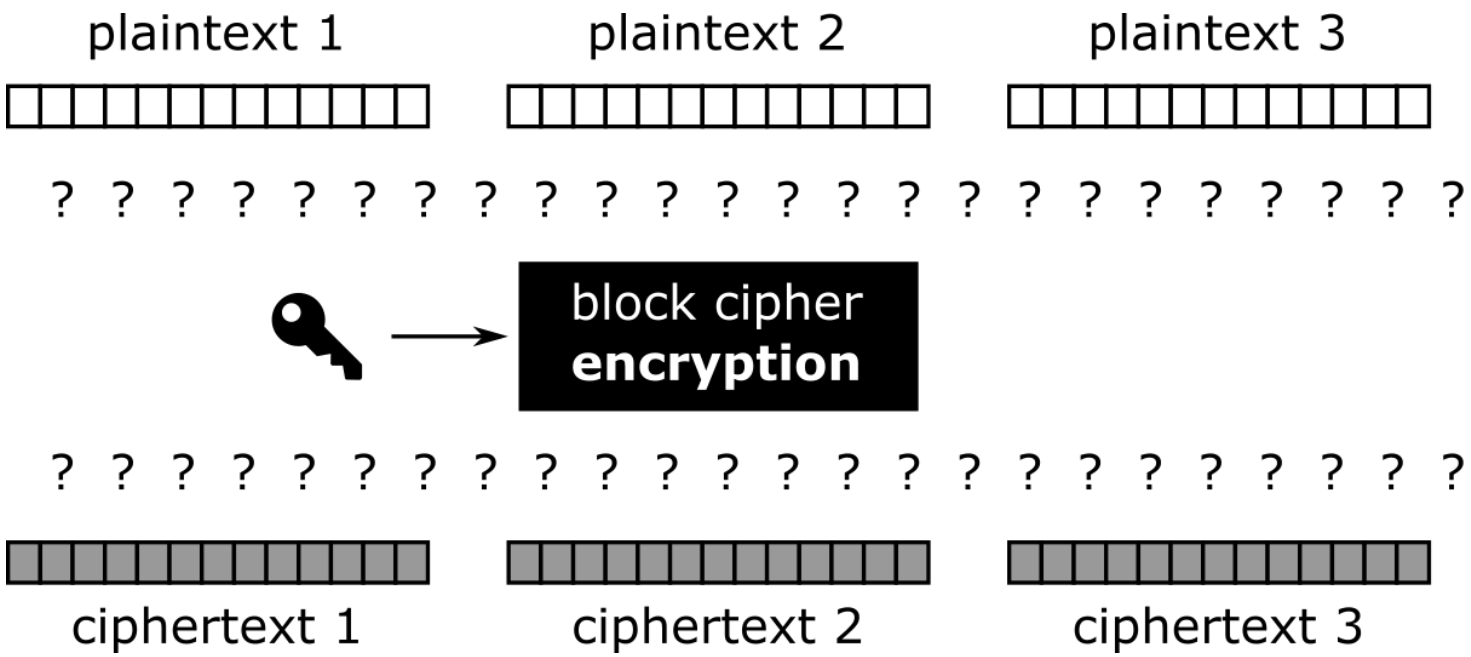
Need for encryption...



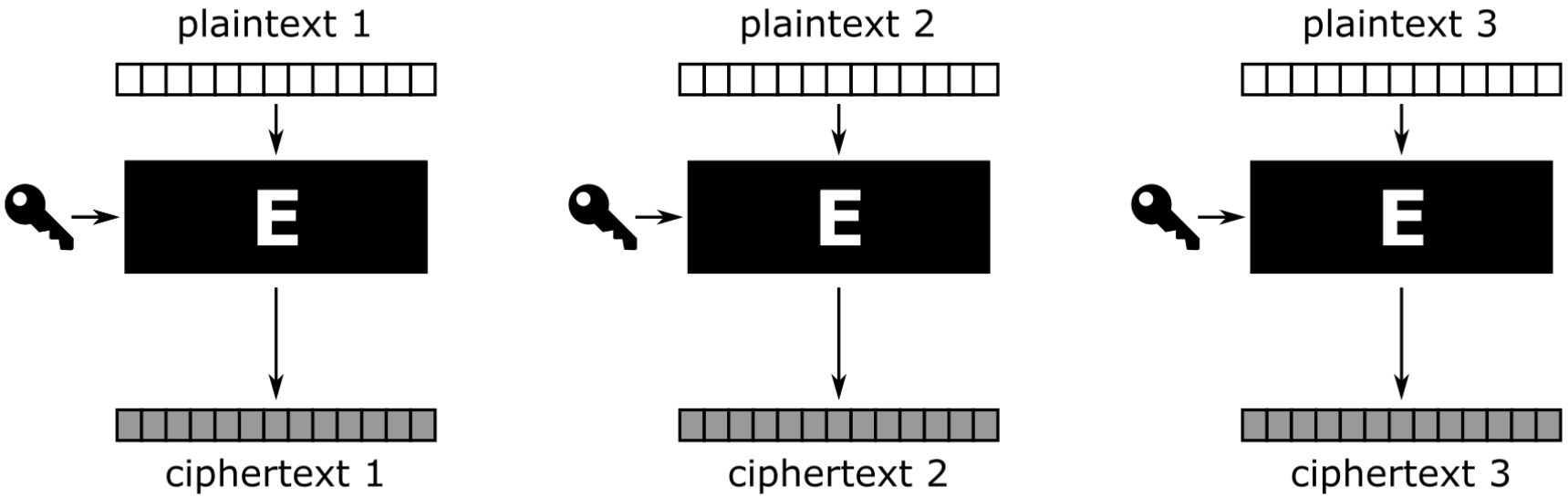
Block cipher to help!



Cutting plaintext in small, workable pieces

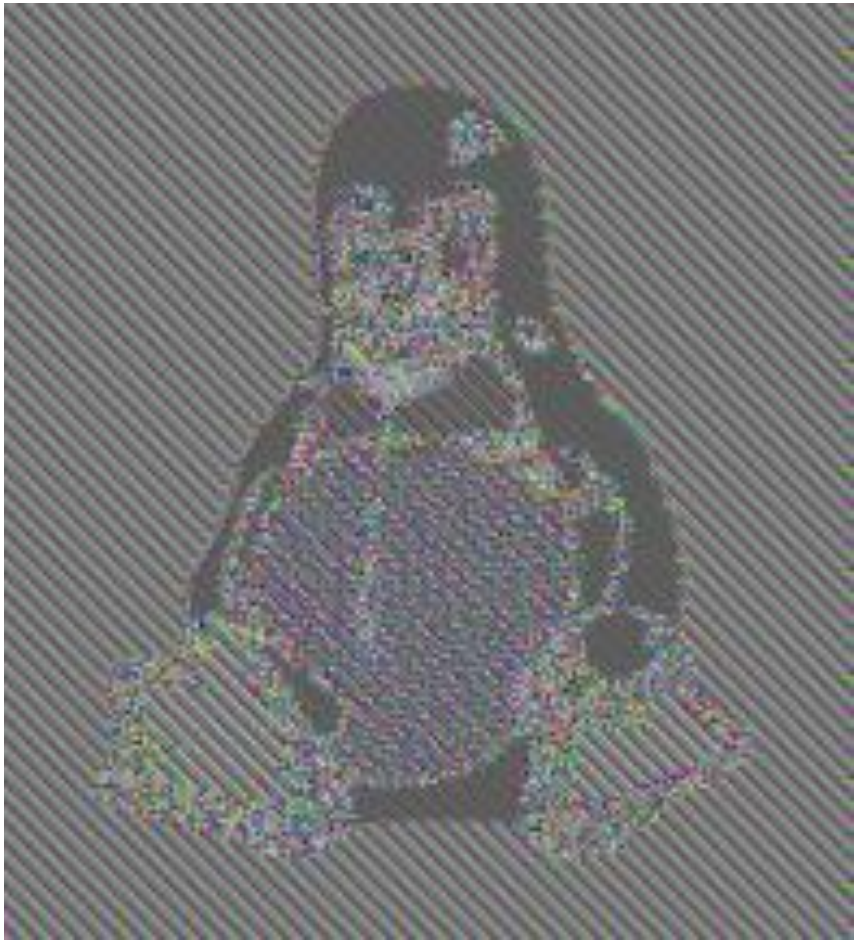


Electronic code book (ECB)

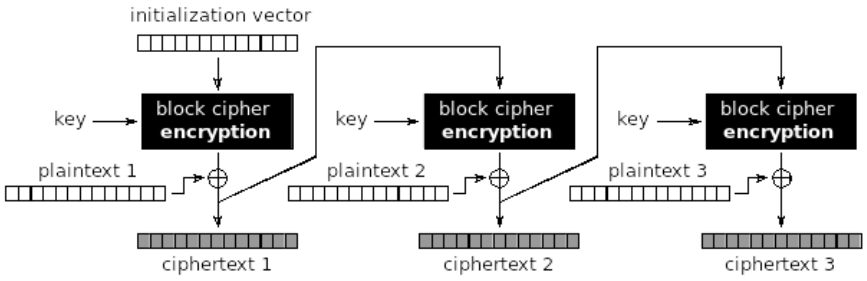


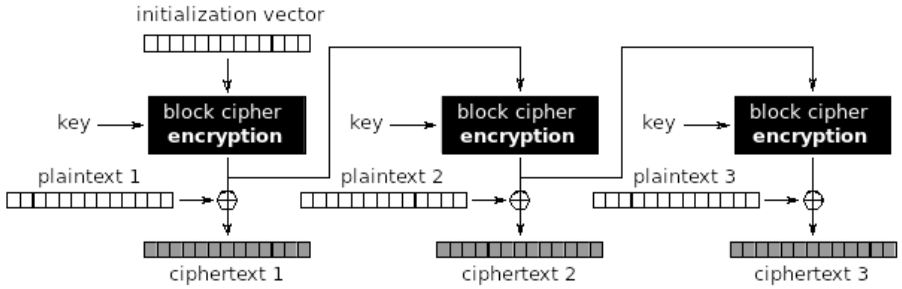
Encrypting TUX (ECB)

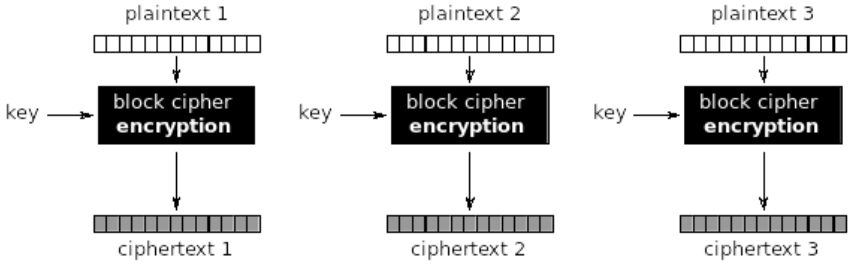
Encrypting TUX (ECB)

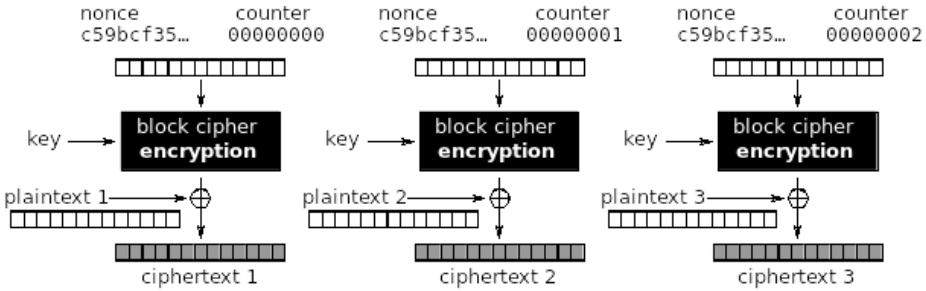


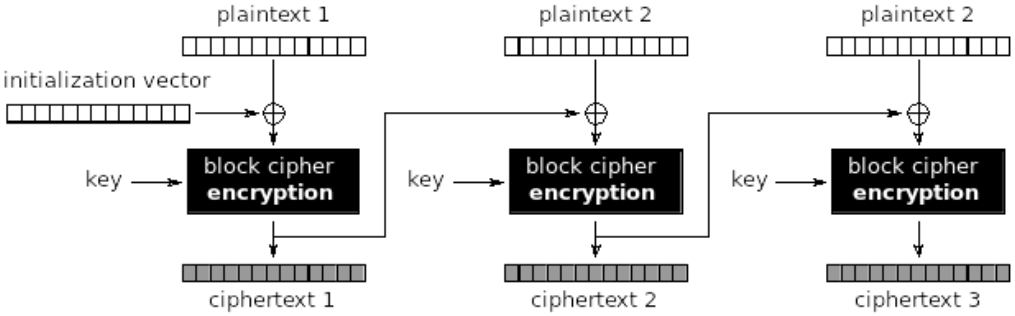
We can do better...











Features of XOR (eXclusive OR)

$$\begin{array}{rcccc} & 0 & 0 & 1 & 1 \\ \oplus & 0 & 1 & 0 & 1 \\ \hline & 0 & 1 & 1 & 0 \end{array}$$

Features of XOR (eXclusive OR)

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

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

Thank you
for your attention.

Questions are welcome!

Martin Ukrop mukrop@mail.muni.cz
Faculty of Informatics, Masaryk University

CROCS
Centre for Research on Cryptography and Security