

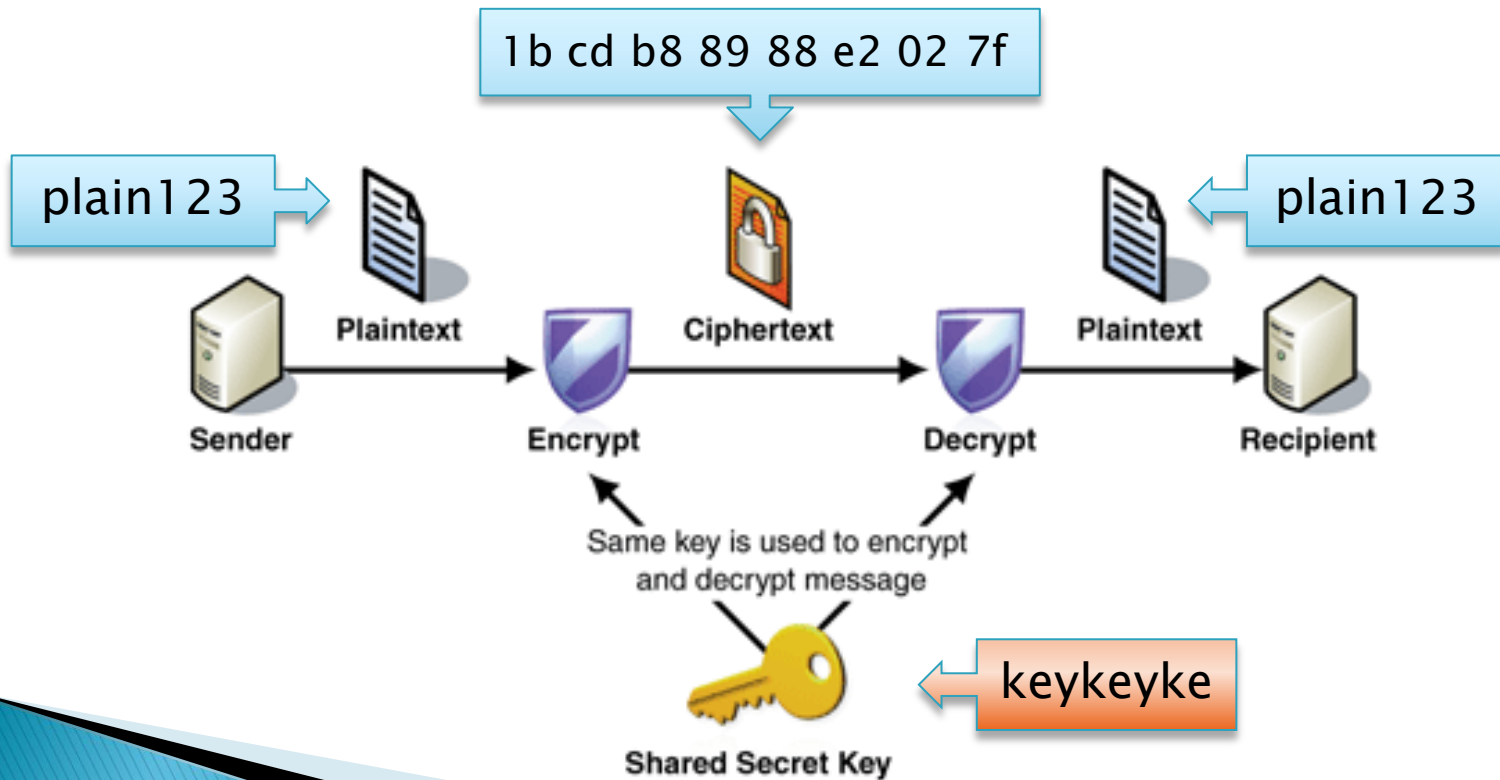


Bruteforcing DES

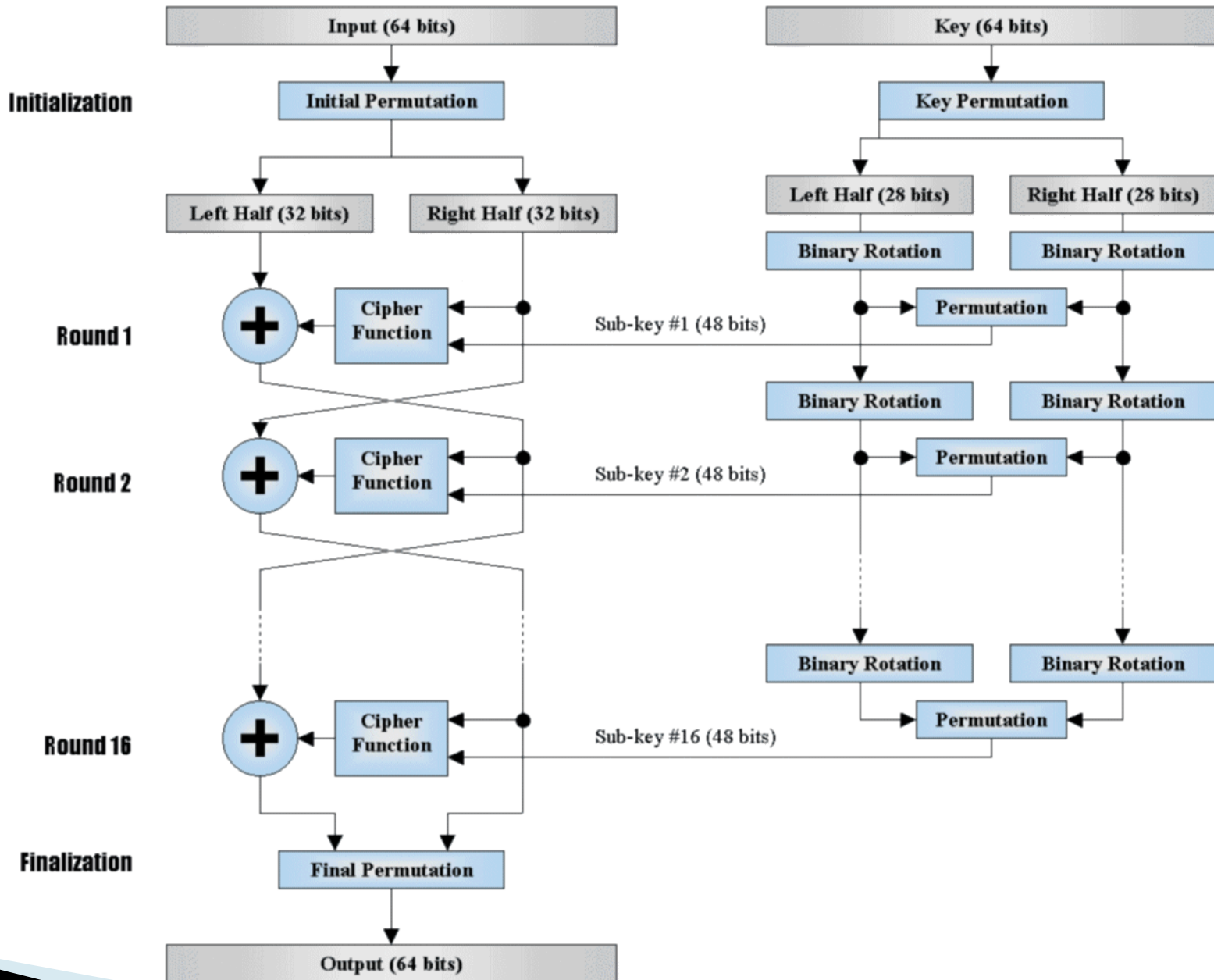
with CUDA on a GPU

What is DES?

- ▶ DES = Data Encryption Standard
- ▶ Symmetric Encryption Algorithm by IBM (1975)

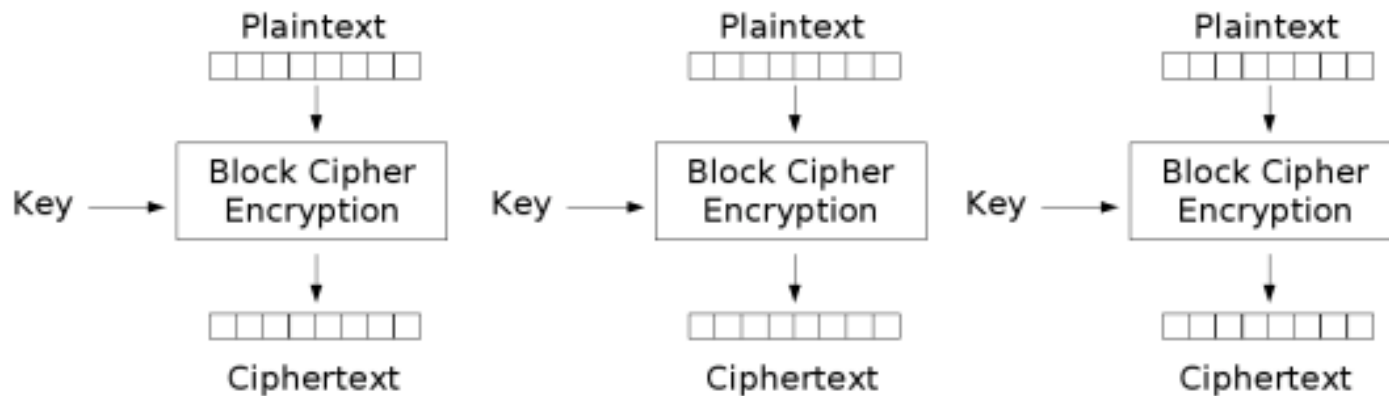


How
does
it
work
?



Modes of operation

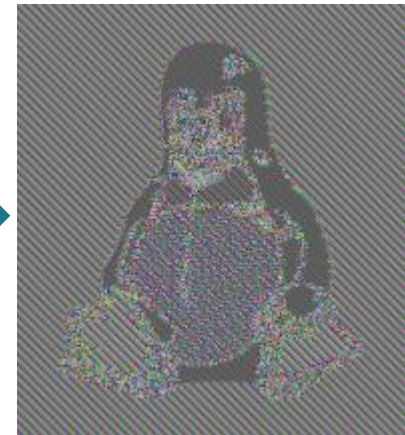
► ECB (Electronic Code Book)



Electronic Codebook (ECB) mode encryption

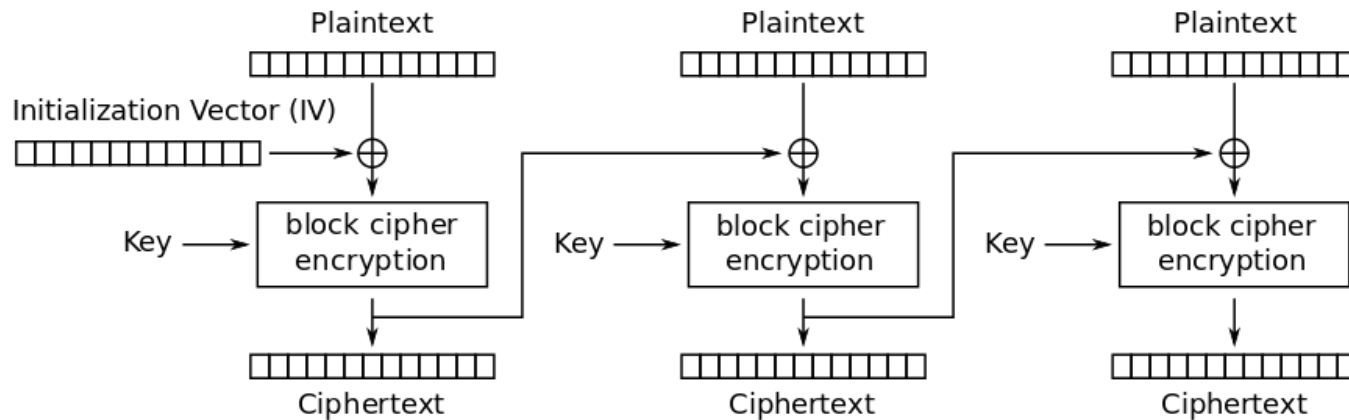
✚ Blocks can be encrypted in parallel

▢ Weak encryption results



Modes of operation

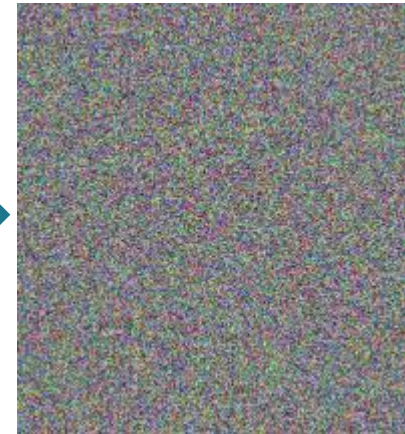
► CBC (Cipher Block Chaining)



Cipher Block Chaining (CBC) mode encryption

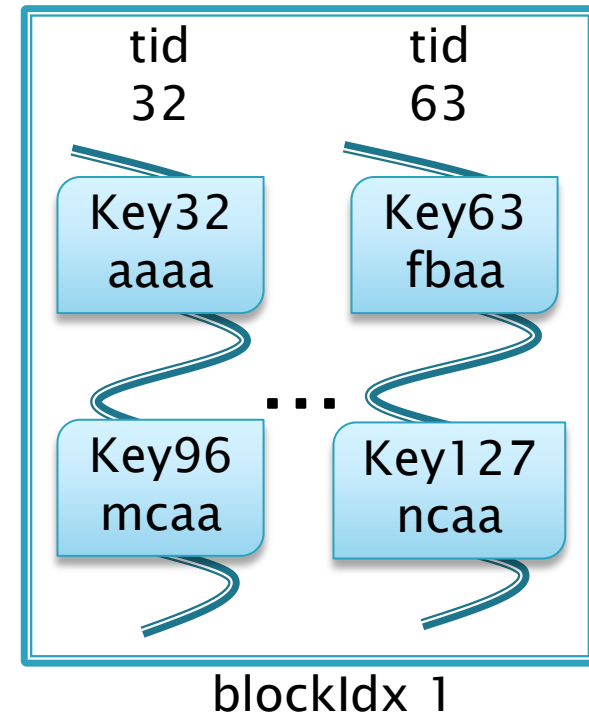
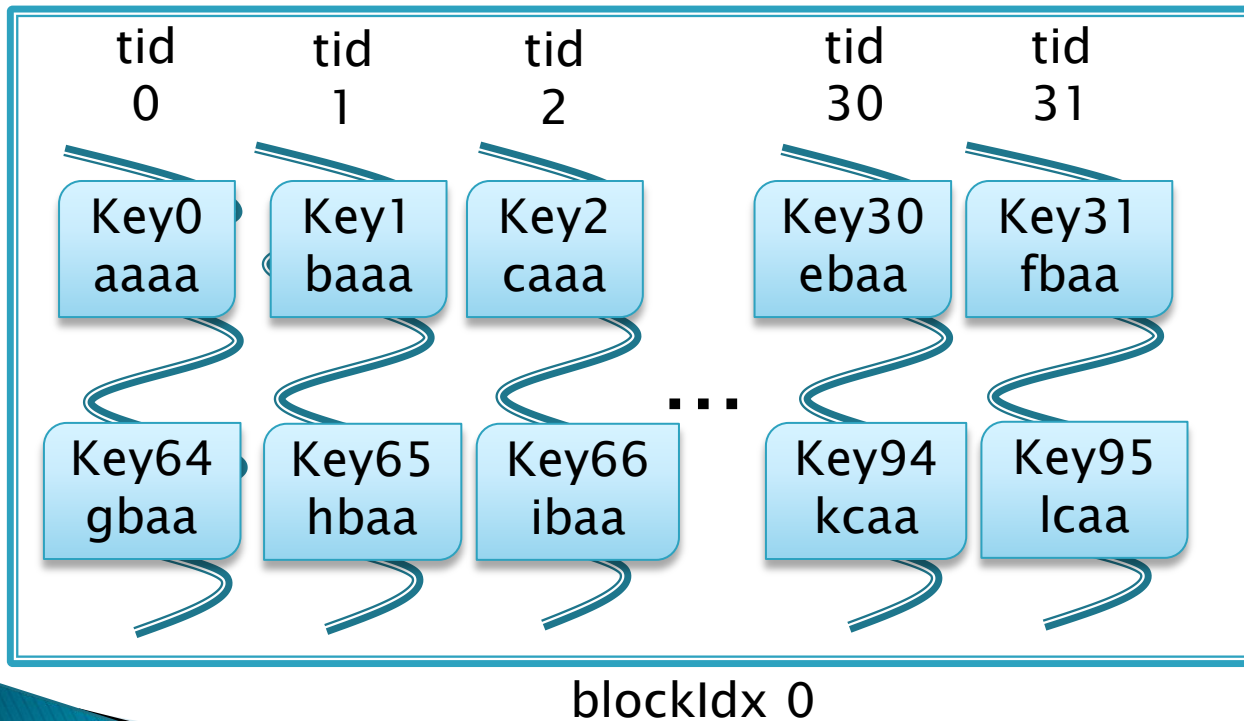
✚ Better encryption results

➡ Not parallelizable



How to bruteforce

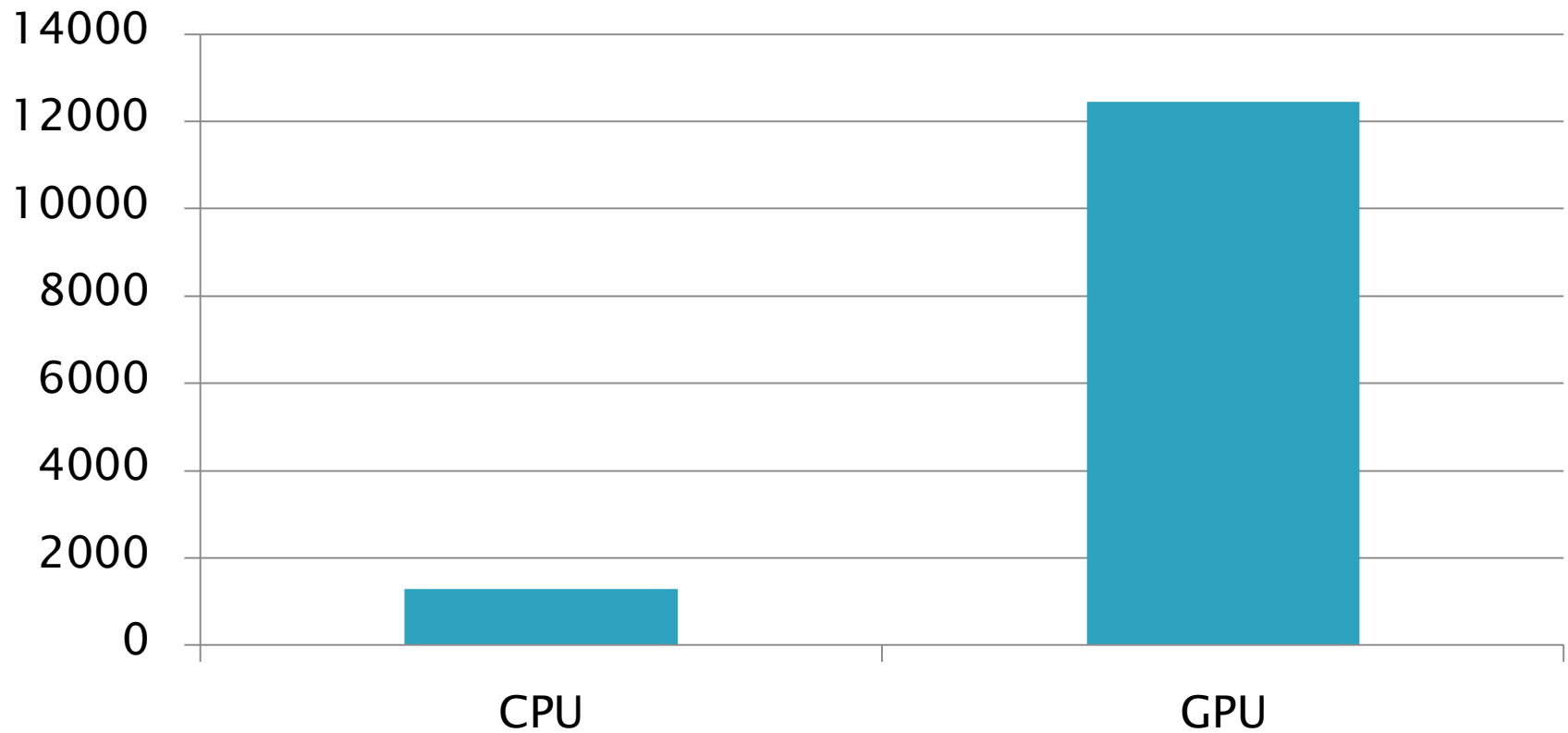
- ▶ CUDA kernels try keys k_i
- ▶ Until $\text{cipher} == \text{enc}_k(\text{plain})$



Each thread tries a different key
and jumps by $\text{blockDim.x} * \text{gridDim.x}$

Performance

Encryption rate [ms^{-1}]



Outlook

- ▶ Optimize parallel code
- ▶ Analyze best combination of threads per block and blocks per grid. (I used 64,32)
- ▶ Utilize multiple cards
- ▶ Use found weakness of DES
 - Keys with distance 1 per byte yield same cipher.
 - Key `keykeyke == jdxjdxjd == jdxkeyje`

**Thank you for
your attention!**

Questions?

