Introduction to Modern Cryptography

4th lecture:
Pseudorandom Functions and Chosen-Plaintext Security

some of these slides are copied from or heavily inspired by the University College London MSc InfoSec 2010 course given by Jens Groth
Thank you very much!
PRG vs PRF

- existence of PRF ⇔ existence of PRG
- both can be based on one-way functions
Battle of Midway (1942)

- important naval battle between the USA and Japan in World War II (Wikipedia)
- decided by cryptographic skills
- US tricked Japanese into acting as encryption oracle
- bottom line: the use of CPA secure encryption could have the course of world history
Battle of Midway Map
Counter (CTR) mode

- CTR mode is CPA-secure if F (the Block Cipher) is a pseudorandom function
- can be precomputed and fully parallelized
- allows random access
Electronic Code Book (ECB)

- highly insecure, should **never** be used
- see example on [wikipedia](https://en.wikipedia.org/wiki/Block_cipher_mode)
Output Feedback (OFB)

• if F is pseudorandom function, then OFB is CPA-secure

• advantage: pseudorandom stream can be precomputed
Cipher Block Chaining (CBC)

• if $F$ is pseudorandom permutation, then CBC is CPA-secure

• drawback: encryption is sequential
BEAST: Browser Exploit Against SSL/TLS

error: reusing the IV of the last-sent CBC block for new connections, see here

treated in this week’s Exercise 3