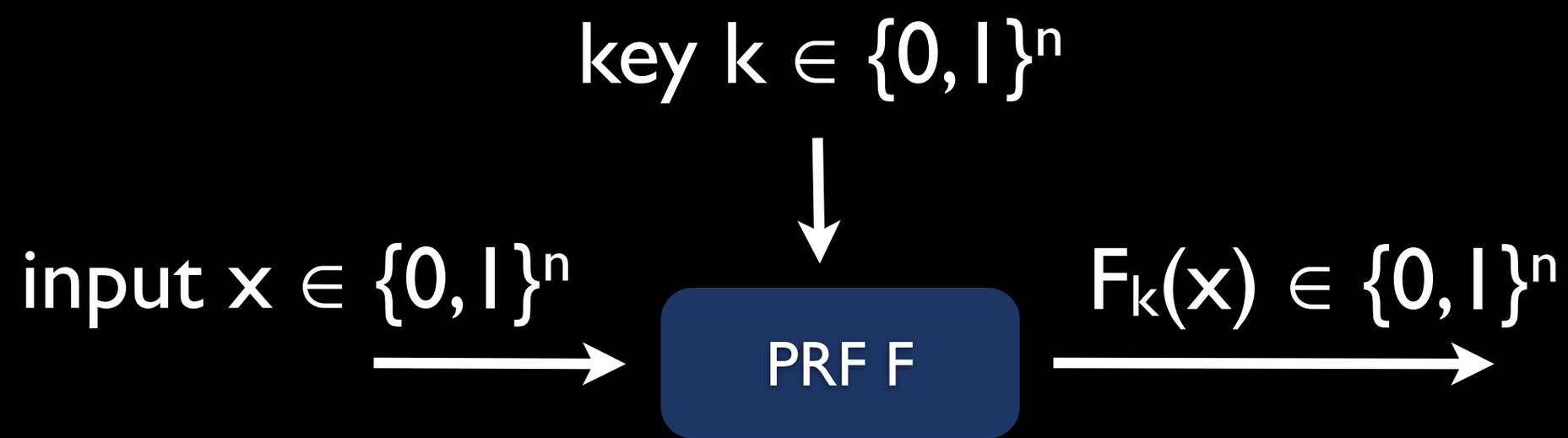
Introduction to Modern Cryptography

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

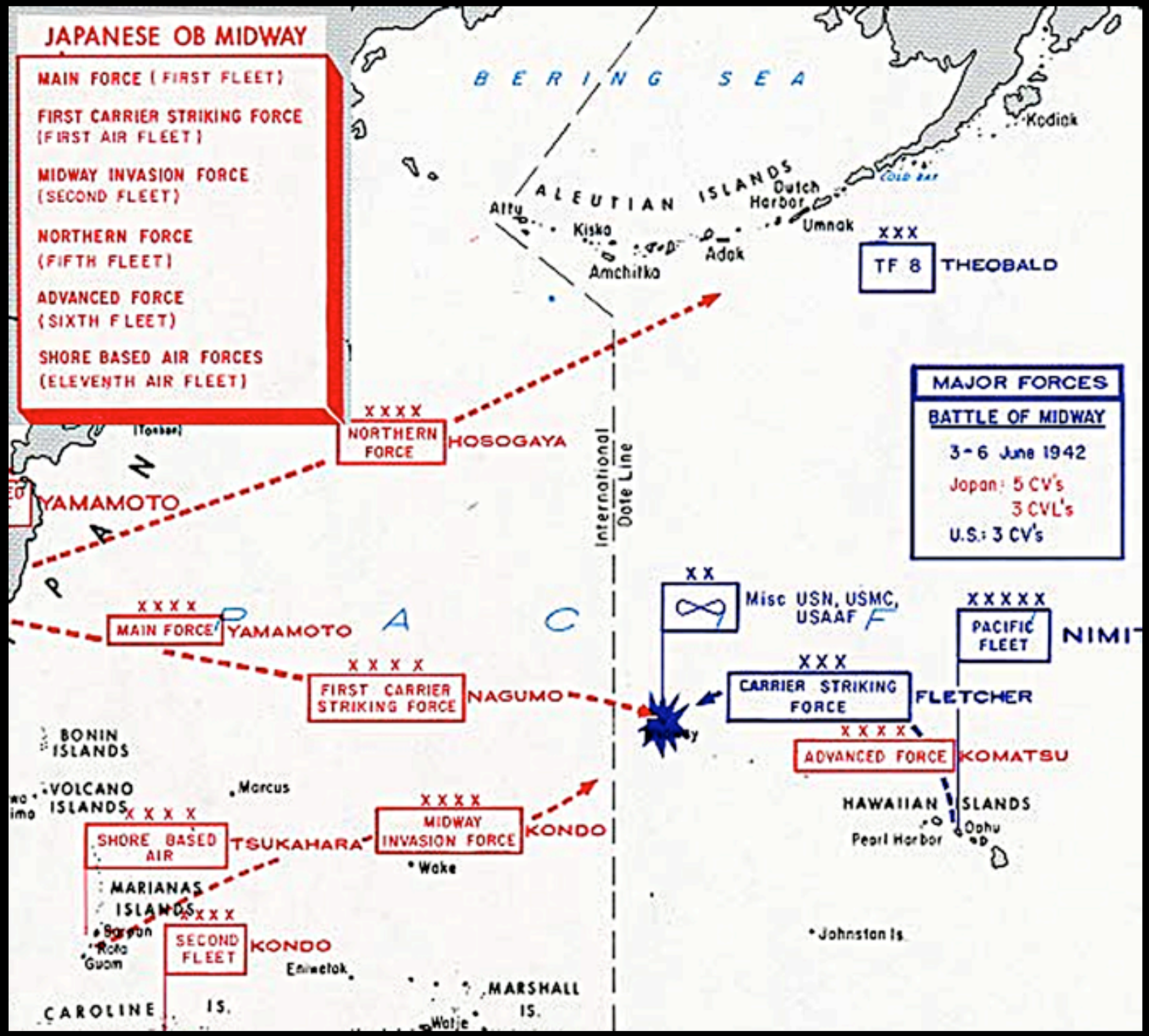


- existence of PRF $\Leftrightarrow$ existence of PRG
- both can be based on one-way functions

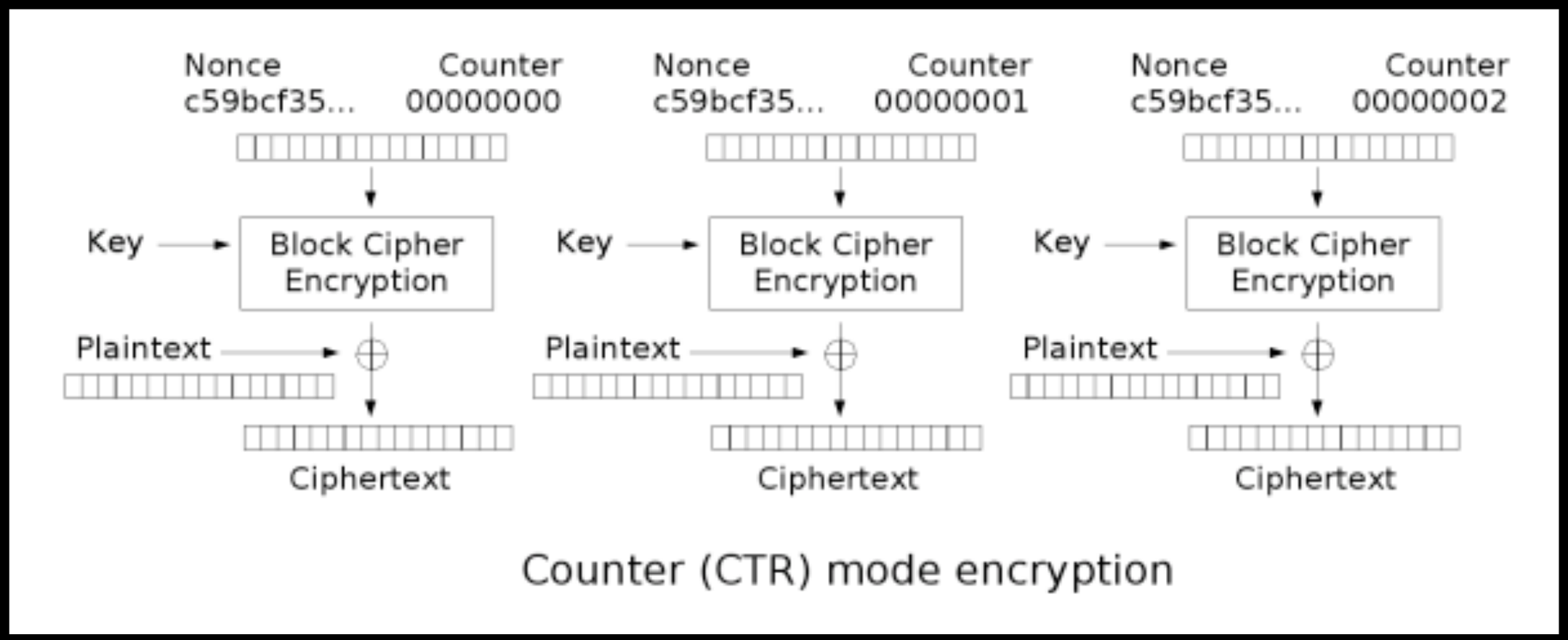
Battle of Midway (1942)

- Midway Atoll: Wikipedia, Google Maps
- 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

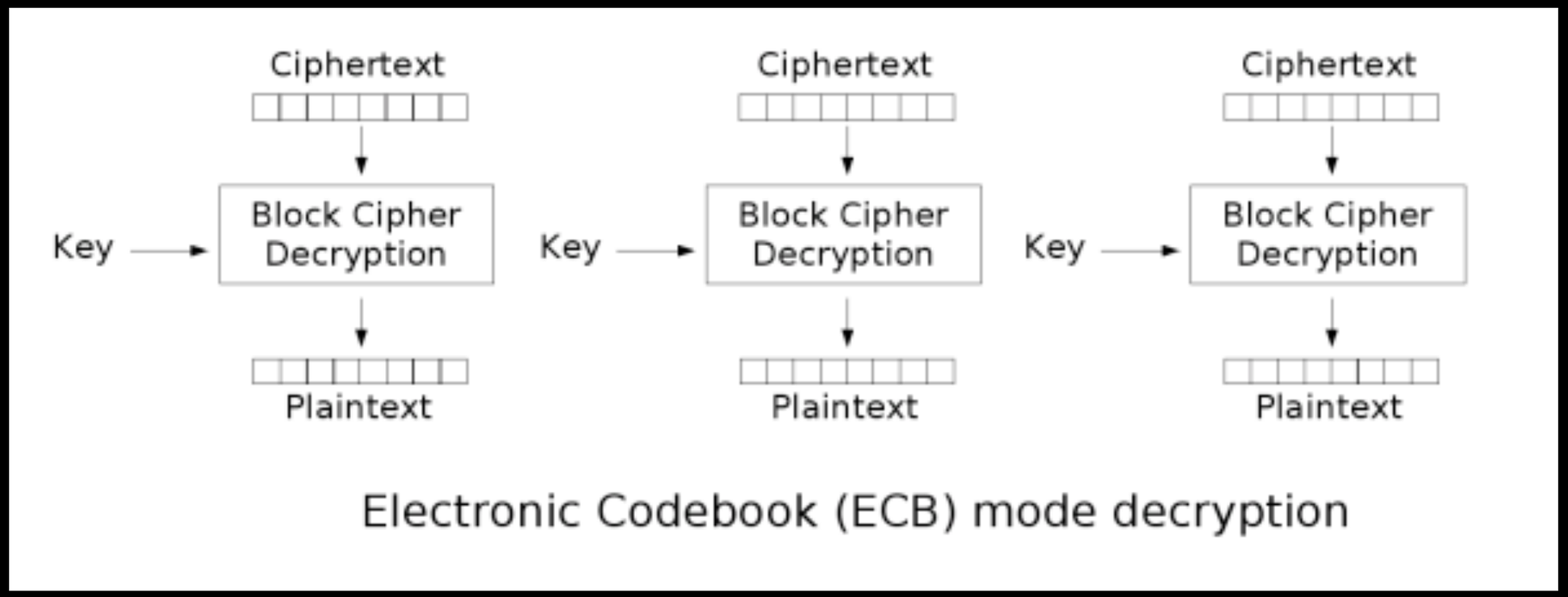


Counter (CTR) mode



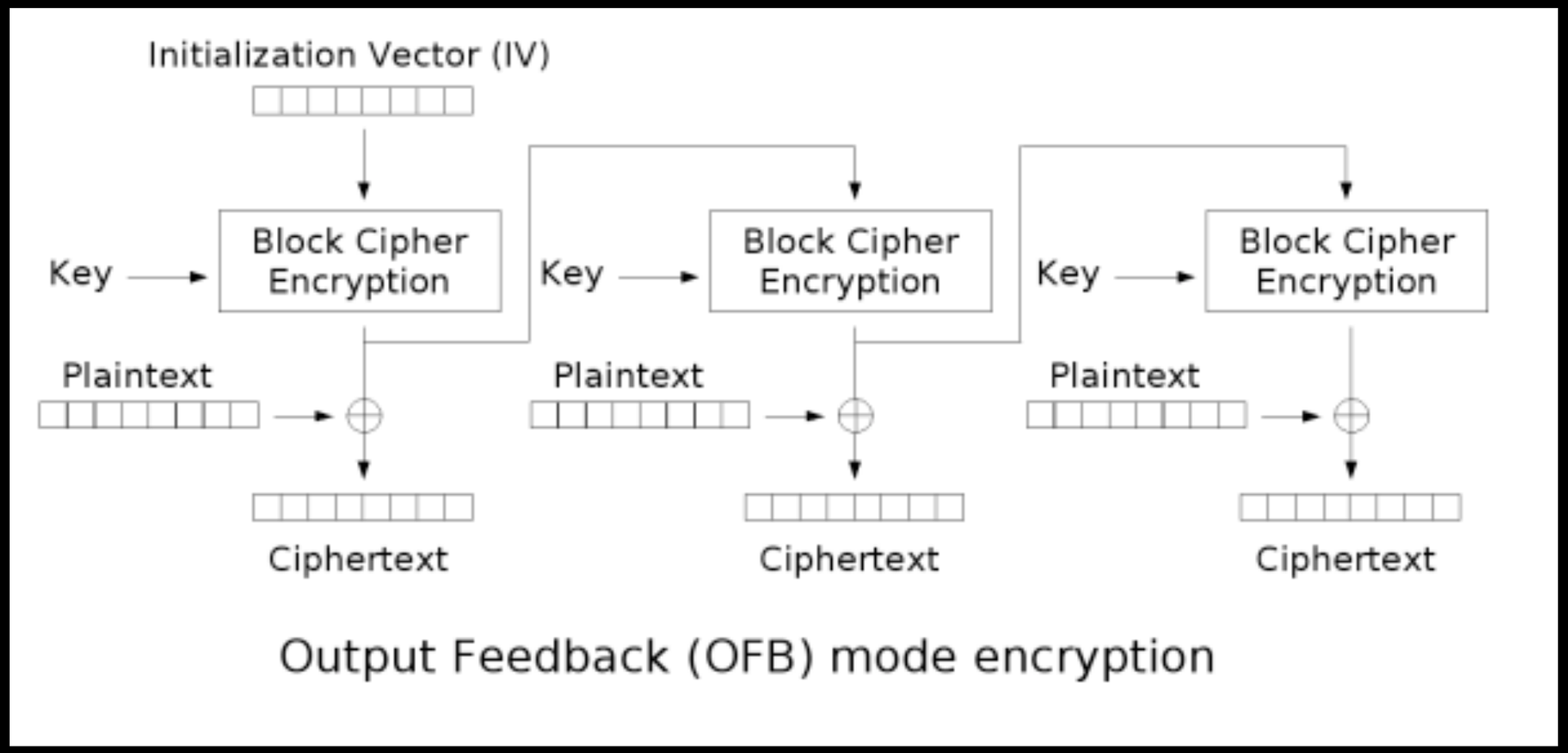
- CTR mode is CPA-secure if F (the Block Cipher) is a pseudorandom function
- can be precomputed and fully parallelized
- allows random access

Electronic Code Book (ECB)



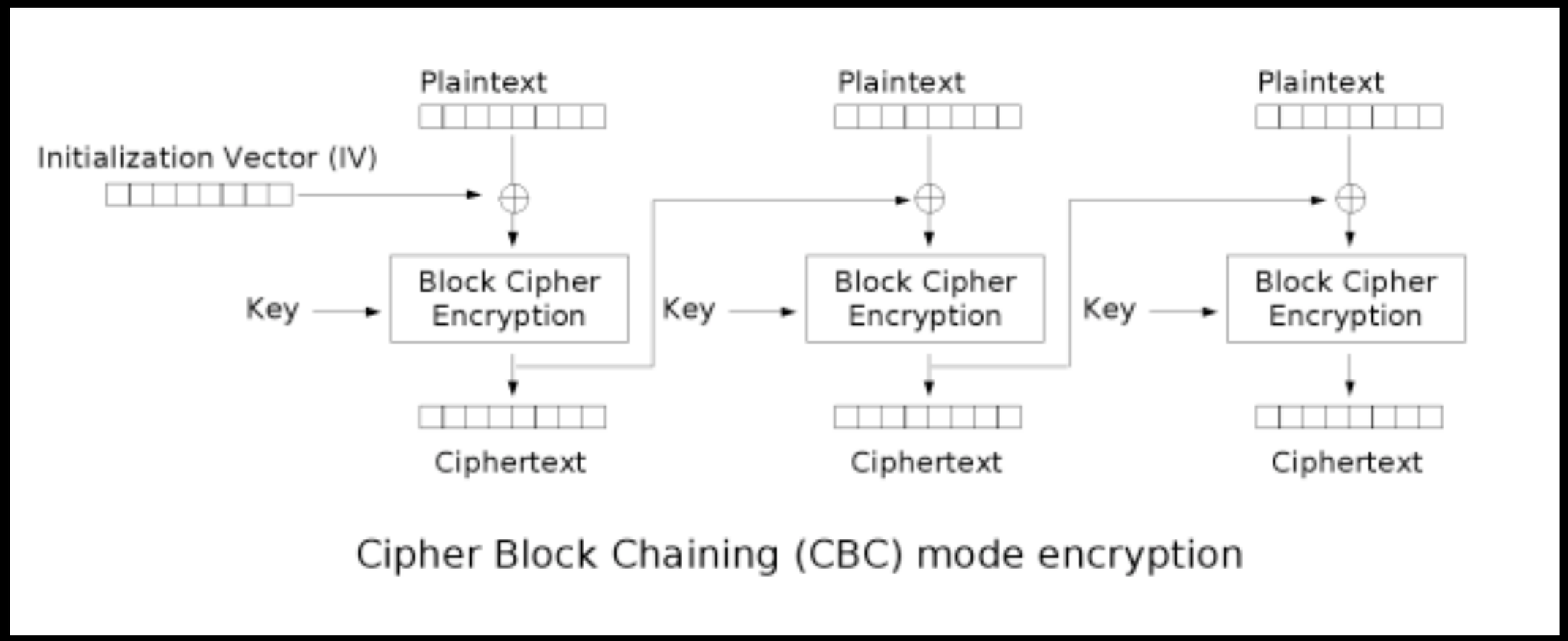
- highly insecure, should never be used
- see example on wikipedia

Output Feedback (OFB)



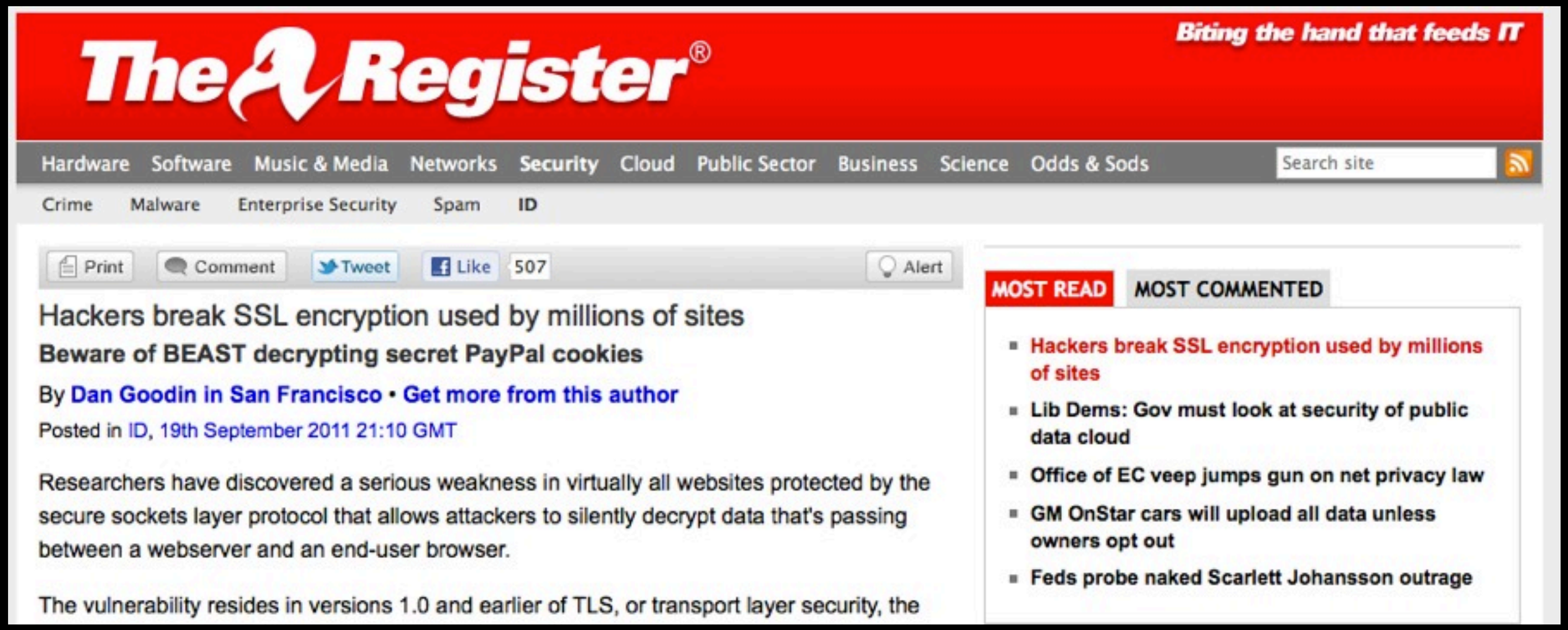
- if F is pseudorandom function, then OFB is CPA-secure
- advantage: pseudorandom stream can be precomputed

Cipher Block Chaining (CBC)



- if F is pseudorandom permutation, then CBC is CPA-secure
- drawback: encryption is sequential

Breaking News (23 Sep 2011)



The Register®

Biting the hand that feeds IT

Hardware Software Music & Media Networks Security Cloud Public Sector Business Science Odds & Sods

Search site

Crime Malware Enterprise Security Spam ID

Print Comment Tweet Like 507 Alert

Hackers break SSL encryption used by millions of sites

Beware of BEAST decrypting secret PayPal cookies

By Dan Goodin in San Francisco • Get more from this author

Posted in ID, 19th September 2011 21:10 GMT

Researchers have discovered a serious weakness in virtually all websites protected by the secure sockets layer protocol that allows attackers to silently decrypt data that's passing between a webserver and an end-user browser.

The vulnerability resides in versions 1.0 and earlier of TLS, or transport layer security, the

MOST READ MOST COMMENTED

- Hackers break SSL encryption used by millions of sites
- Lib Dems: Gov must look at security of public data cloud
- Office of EC veep jumps gun on net privacy law
- GM OnStar cars will upload all data unless owners opt out
- Feds probe naked Scarlett Johansson outrage

- 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