Introduction to Modern Cryptography

4th lecture:

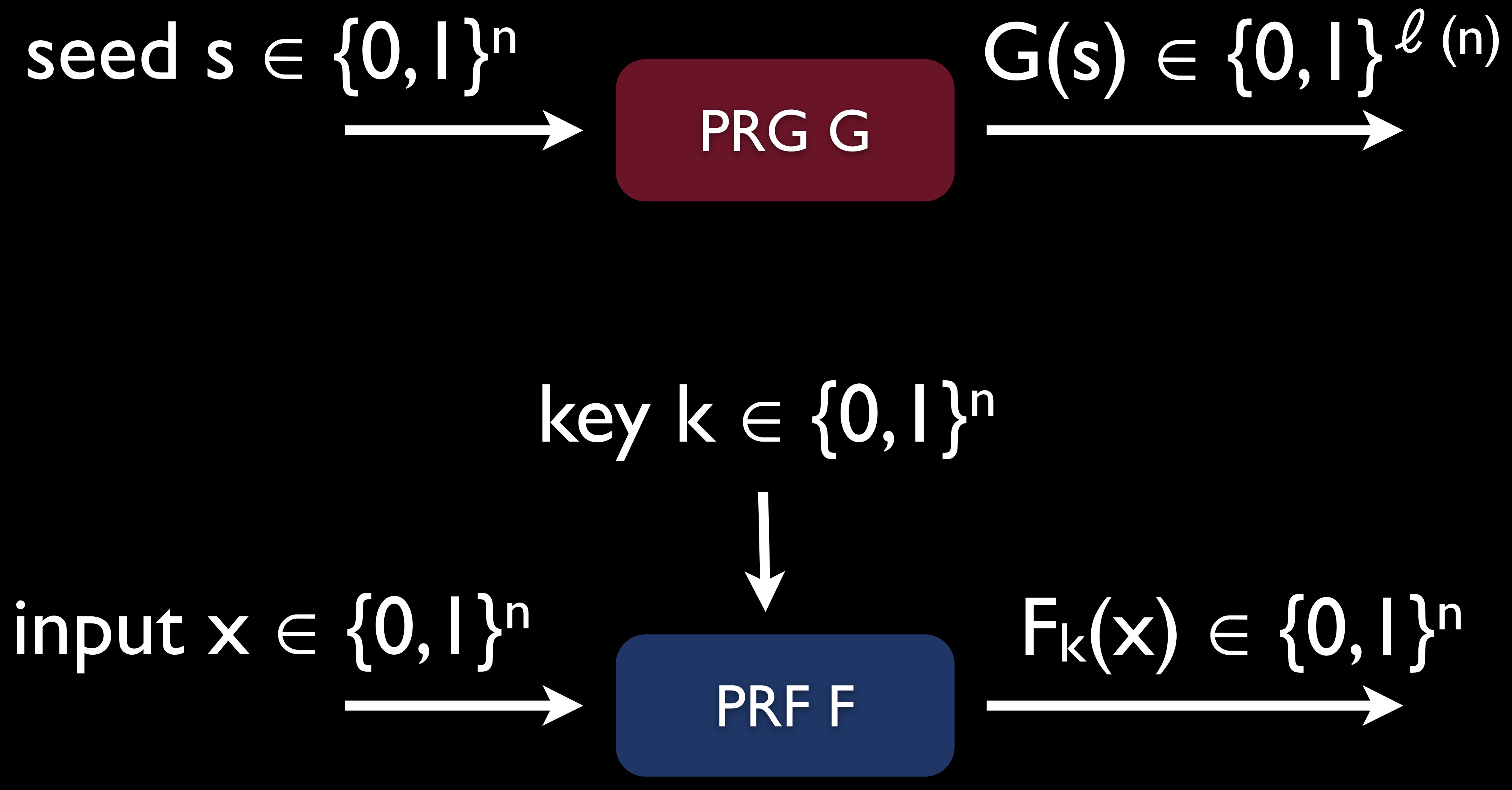
Pseudorandom Functions and Chosen-Plaintext Security last time:

- computational security
- pseudorandomness
- reduction proof

4th lecture (today):

- pseudorandom functions
- chosen-plaintext security

PRG vs PRF



seed $s \in \{0,1\}^n$

PRG G

$G(s) \in \{0,1\}^{\ell(n)}$

key $k \in \{0,1\}^n$

input $x \in \{0,1\}^n$

PRF F

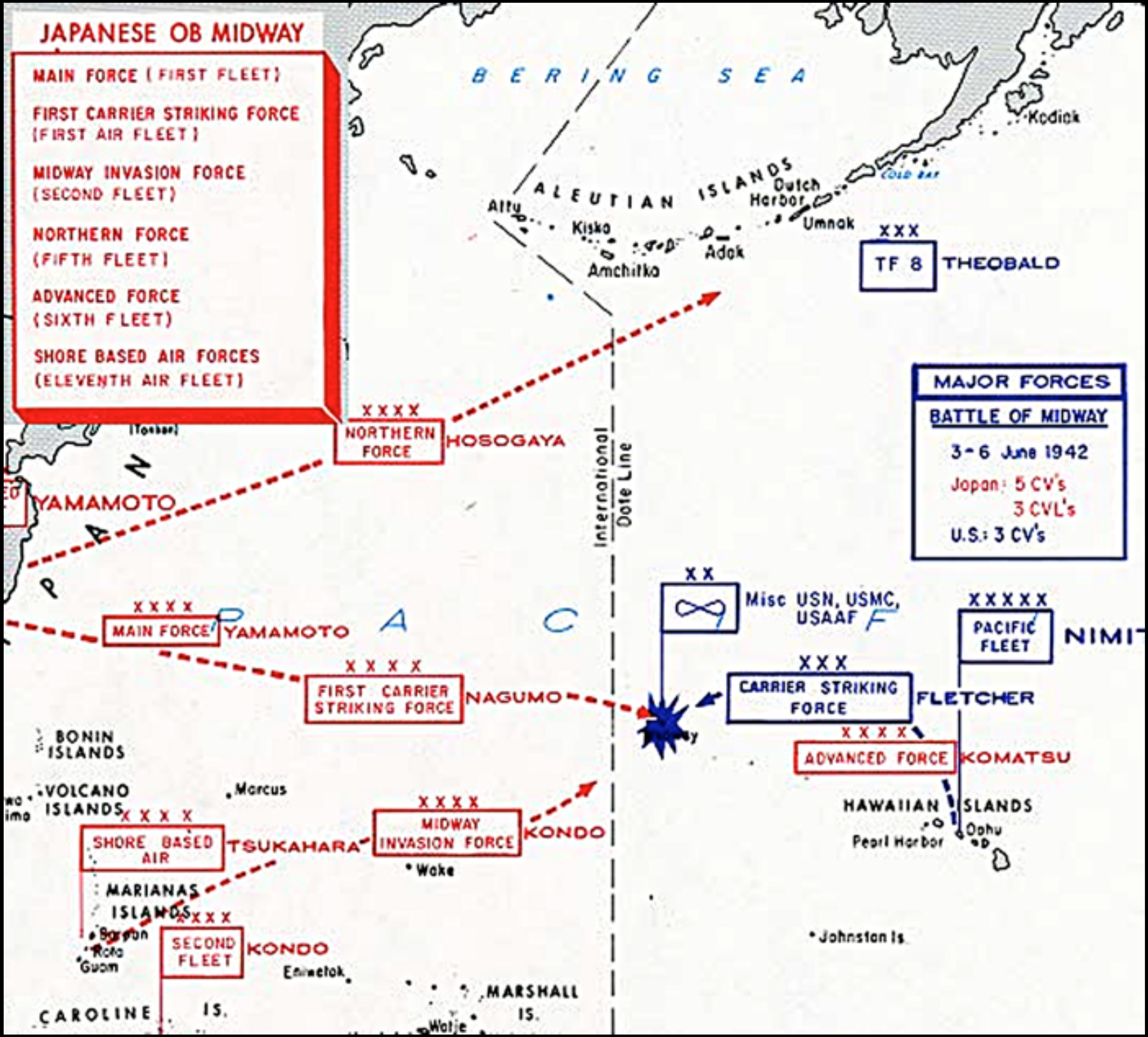
$F_k(x) \in \{0,1\}^n$

- existence of PRF ⇔ existence of PRG
- both can be based on one-way functions

Battle of Midway (1942)

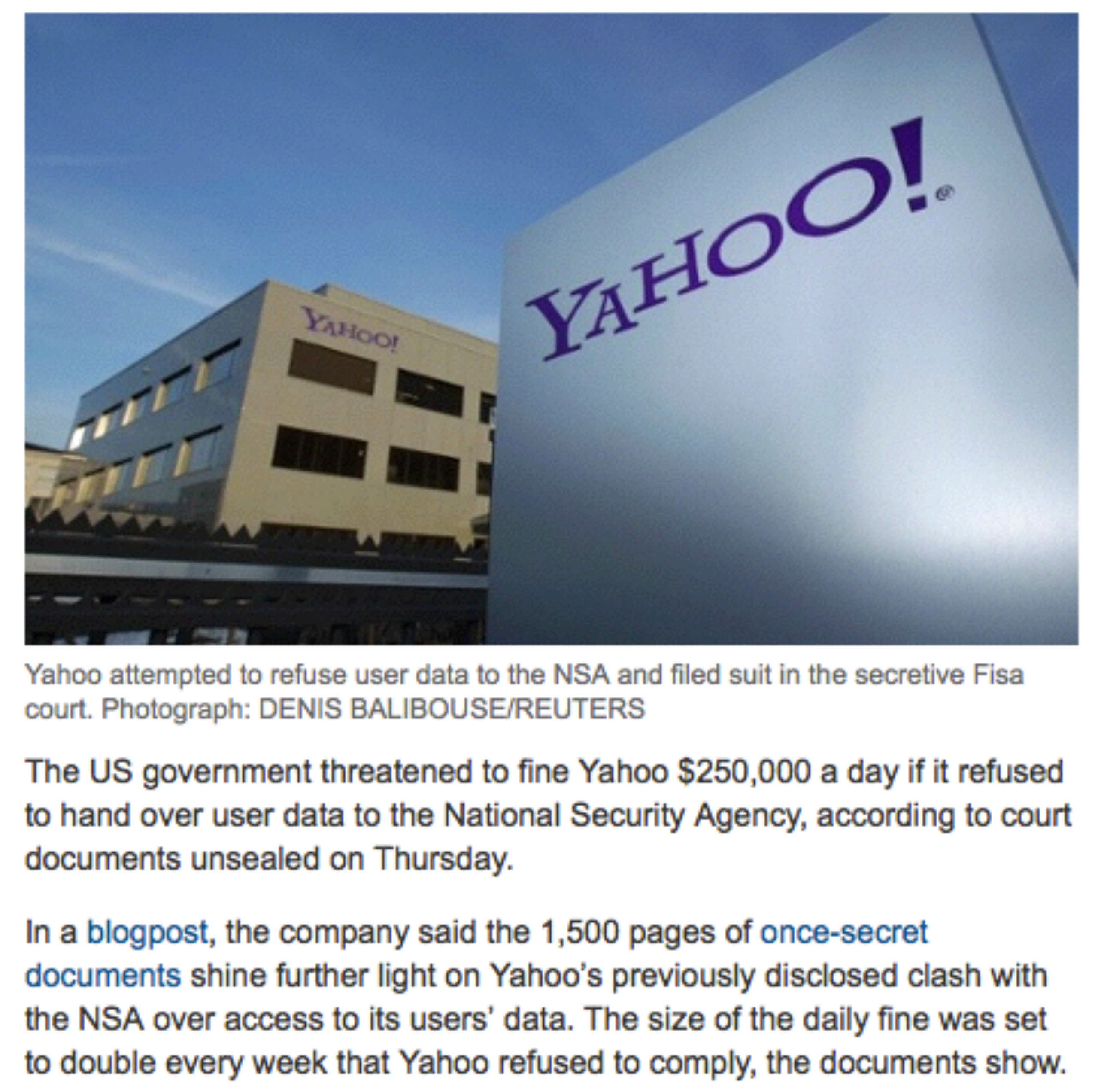
- Midway Atoll: Wikipedia, Google Maps
- important naval battle between the USA and Japan in World War II (Wikipedia)
- decided by cryptographic skills
- US tricked Japanese into acting as encryption oracle
- bottom line: the use of CPA secure encryption could have changed the course of world history

Battle of Midway Map



Last week's NSA news

- On Thu, 11 Sep 2014, Yahoo posted this article on their blog. Read the news here.
- Wikipedia on the FISC court



Yahoo attempted to refuse user data to the NSA and filed suit in the secretive Fisa court. Photograph: DENIS BALIBOUSE/REUTERS

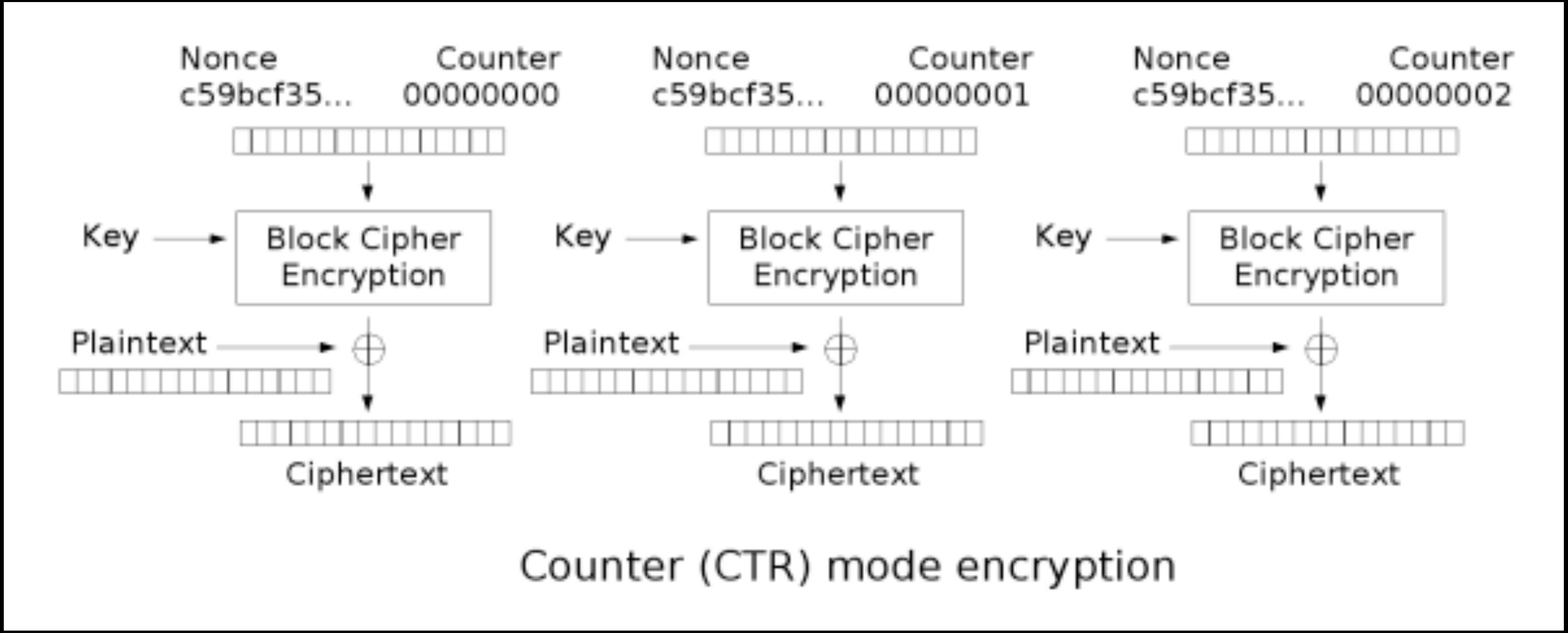
The US government threatened to fine Yahoo $250,000 a day if it refused to hand over user data to the National Security Agency, according to court documents unsealed on Thursday.

In a blogpost, the company said the 1,500 pages of once-secret documents shine further light on Yahoo's previously disclosed clash with the NSA over access to its users' data. The size of the daily fine was set to double every week that Yahoo refused to comply, the documents show.

Last week's NSA news II

- Treasure Map: The NSA Breach of Telekom and Other German Firms
- read the article Spiegel Online

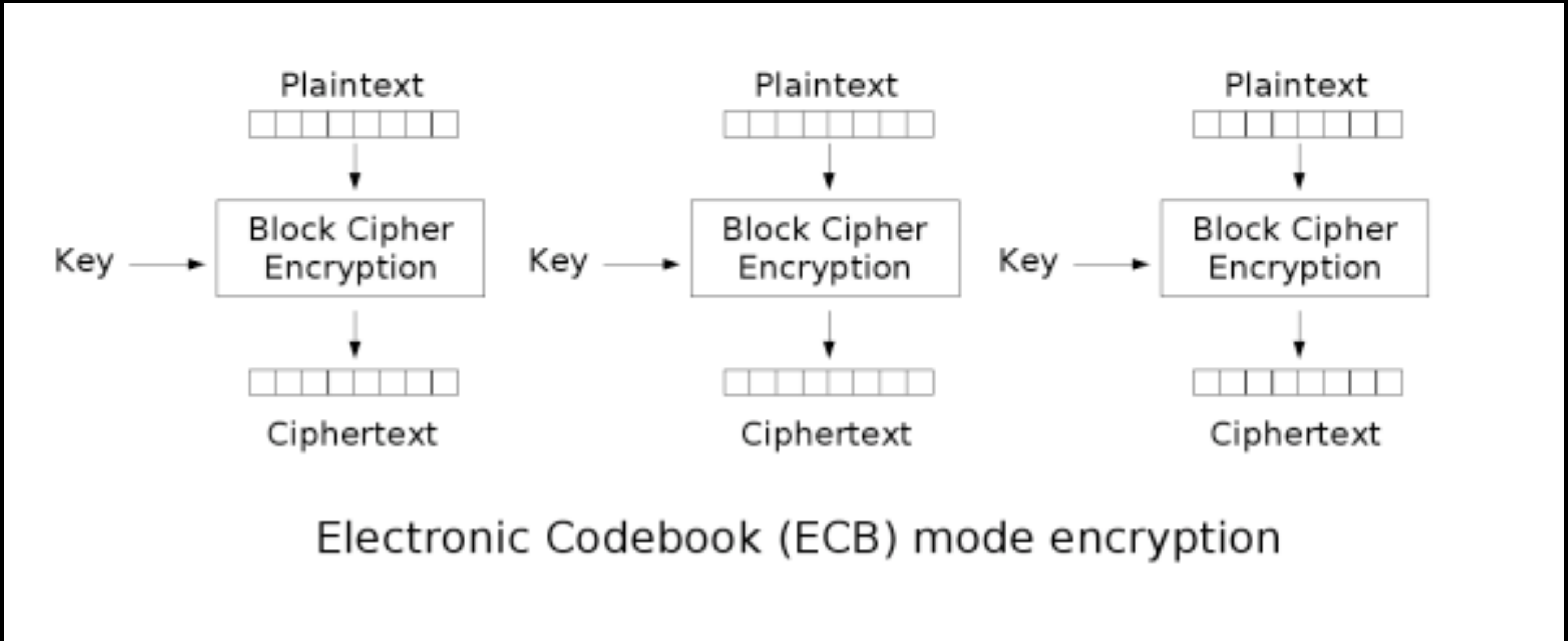
Counter (CTR) mode



Counter (CTR) mode encryption

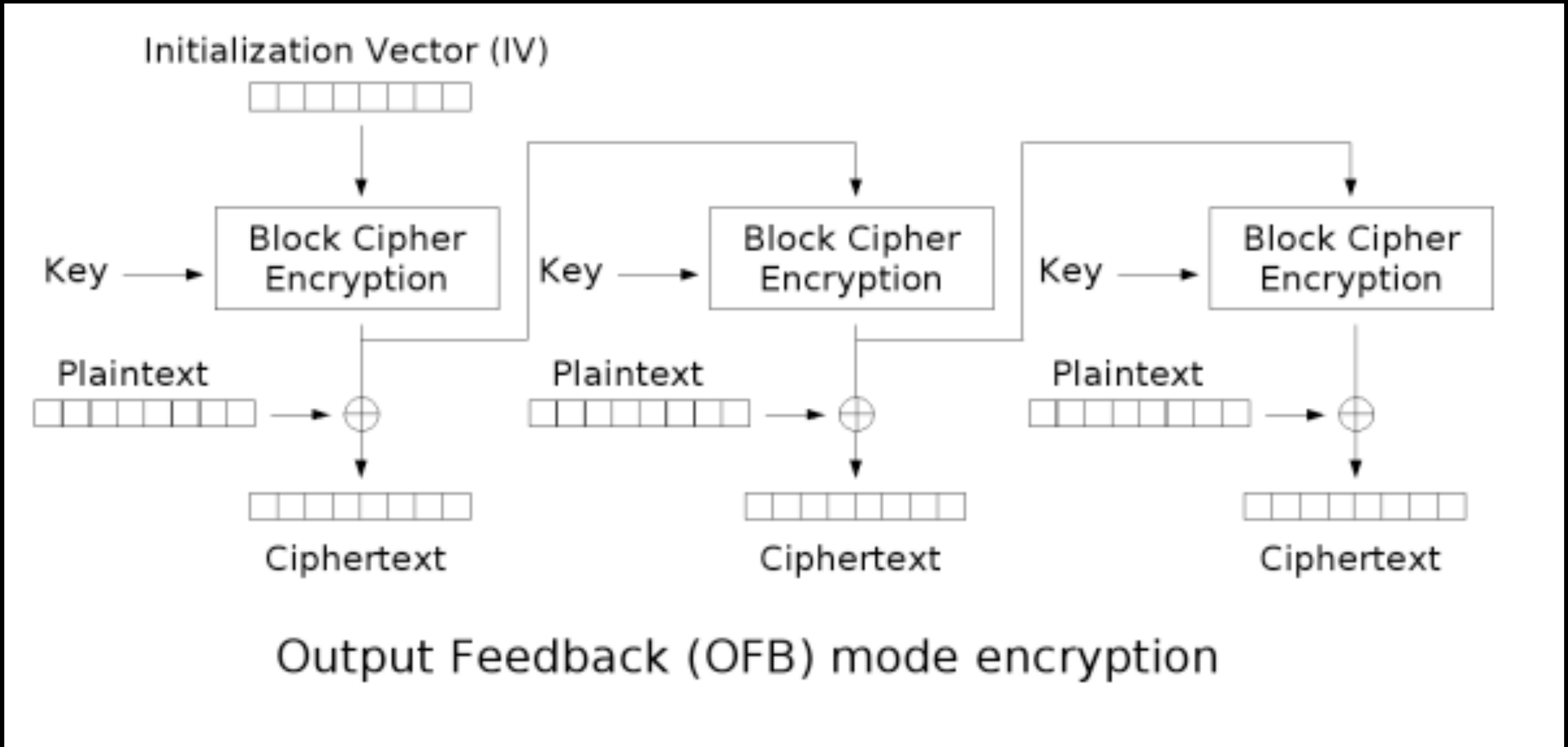
- CTR mode is CPA-secure if F (the Block Cipher) is a pseudorandom function
- can be precomputed and fully parallelized
- allows random access

Electronic Code Book (ECB)



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

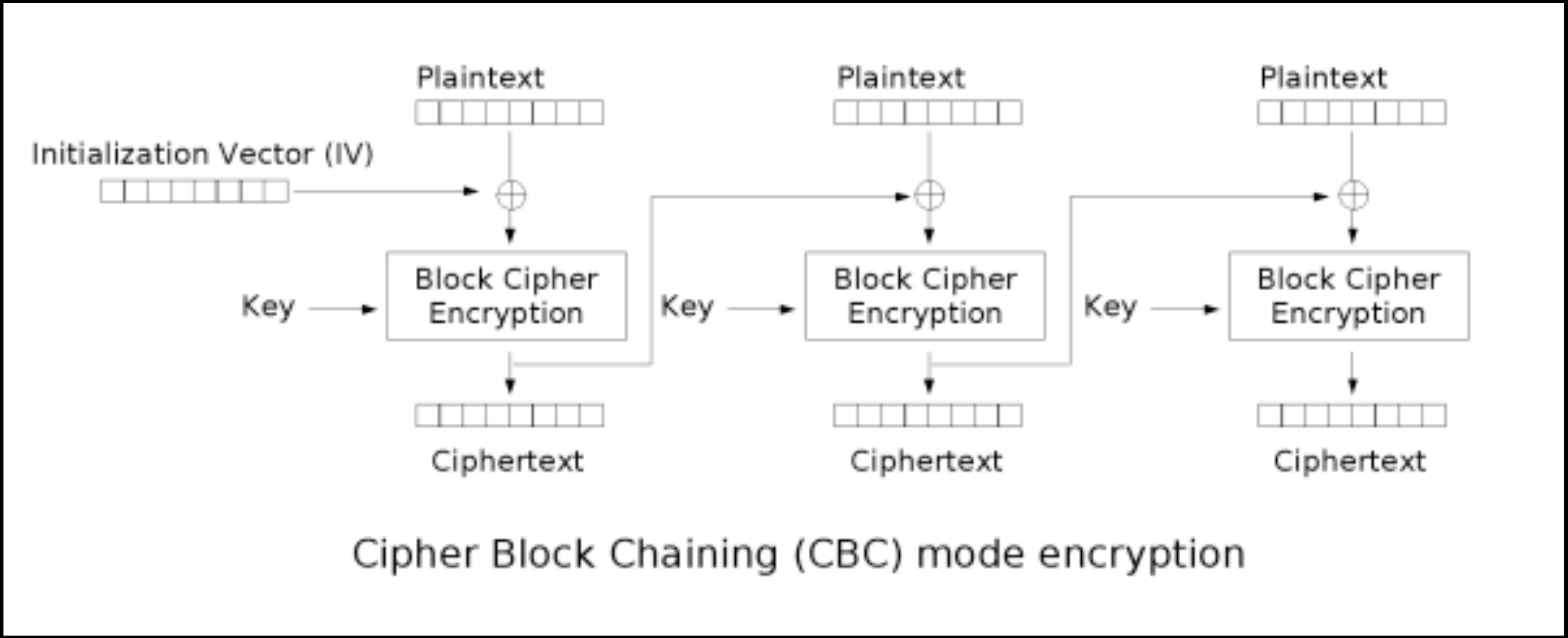
Output Feedback (OFB)



Output Feedback (OFB) mode encryption

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

Cipher Block Chaining (CBC)



Cipher Block Chaining (CBC) mode encryption

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