

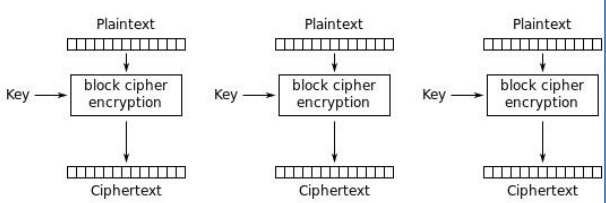
Secure and Efficient Format Preserving Encryption

FSE 2014 Rump Session

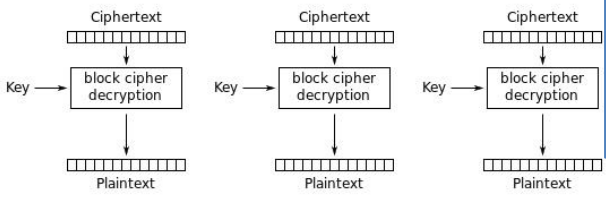
Center for Information Security Technologies (CIST),
Korea University

HyungChul Kang

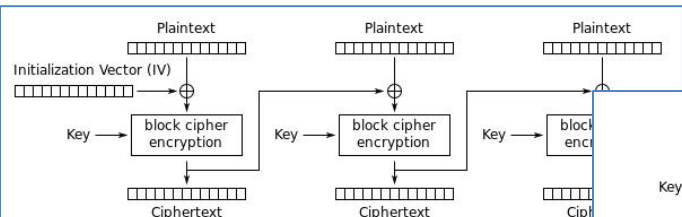
Mode of Operation



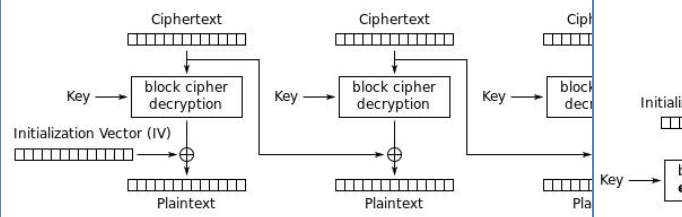
Electronic Codebook (ECB) mode encryption



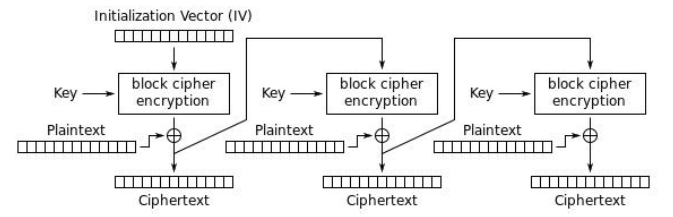
Electronic Codebook (ECB) mode decryption



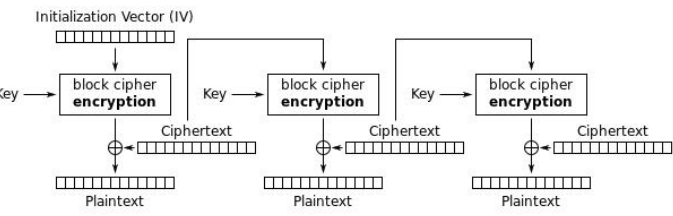
Cipher Block Chaining (CBC) mode encryption



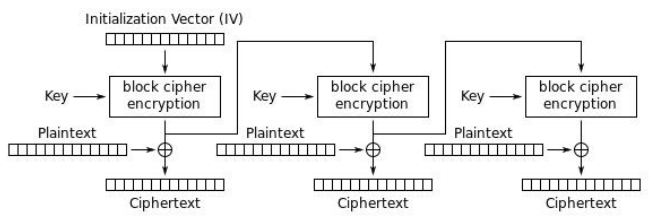
Cipher Block Chaining (CBC) mode decryption



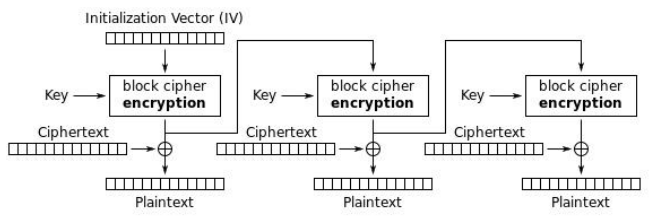
Cipher Feedback (CFB) mode encryption



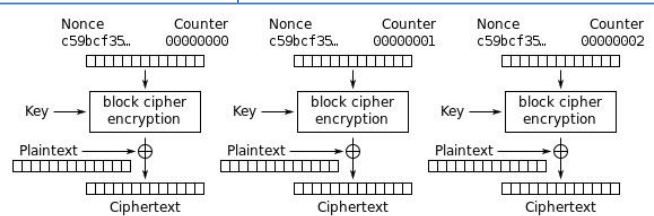
Cipher Feedback (CFB) mode decryption



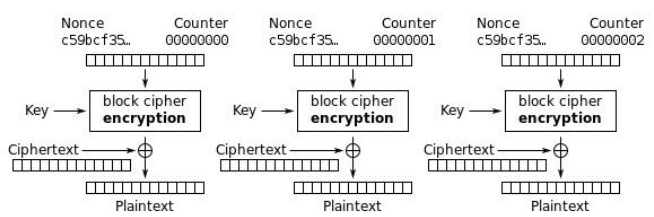
Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption



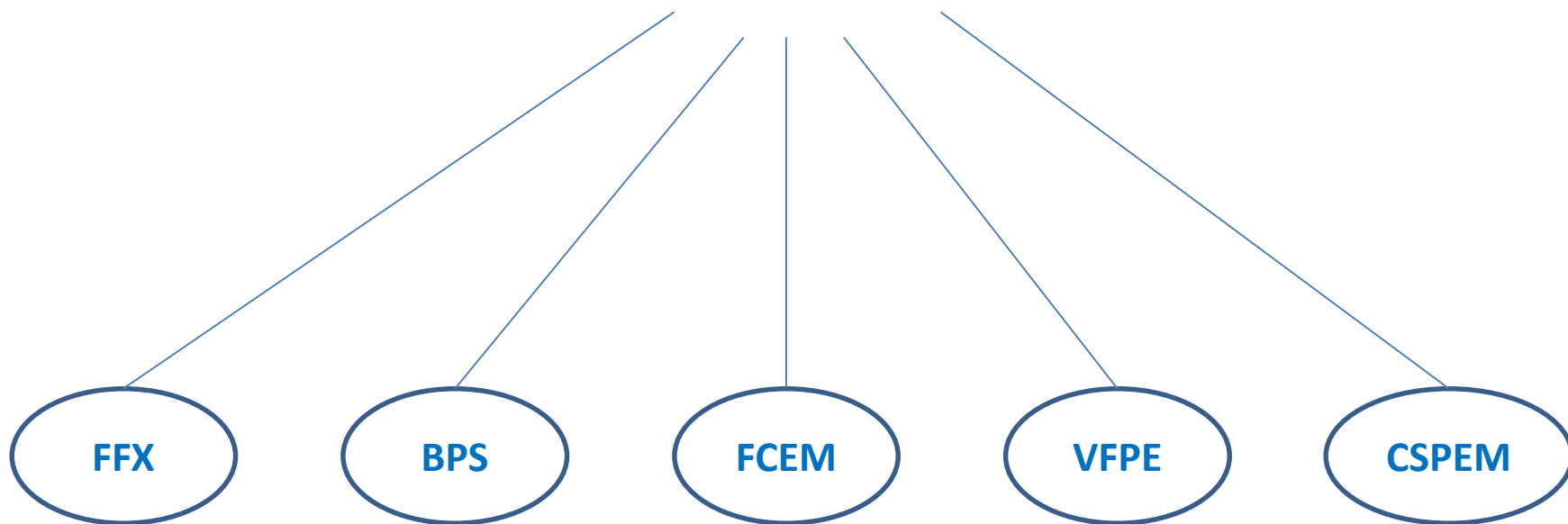
Counter (CTR) mode encryption



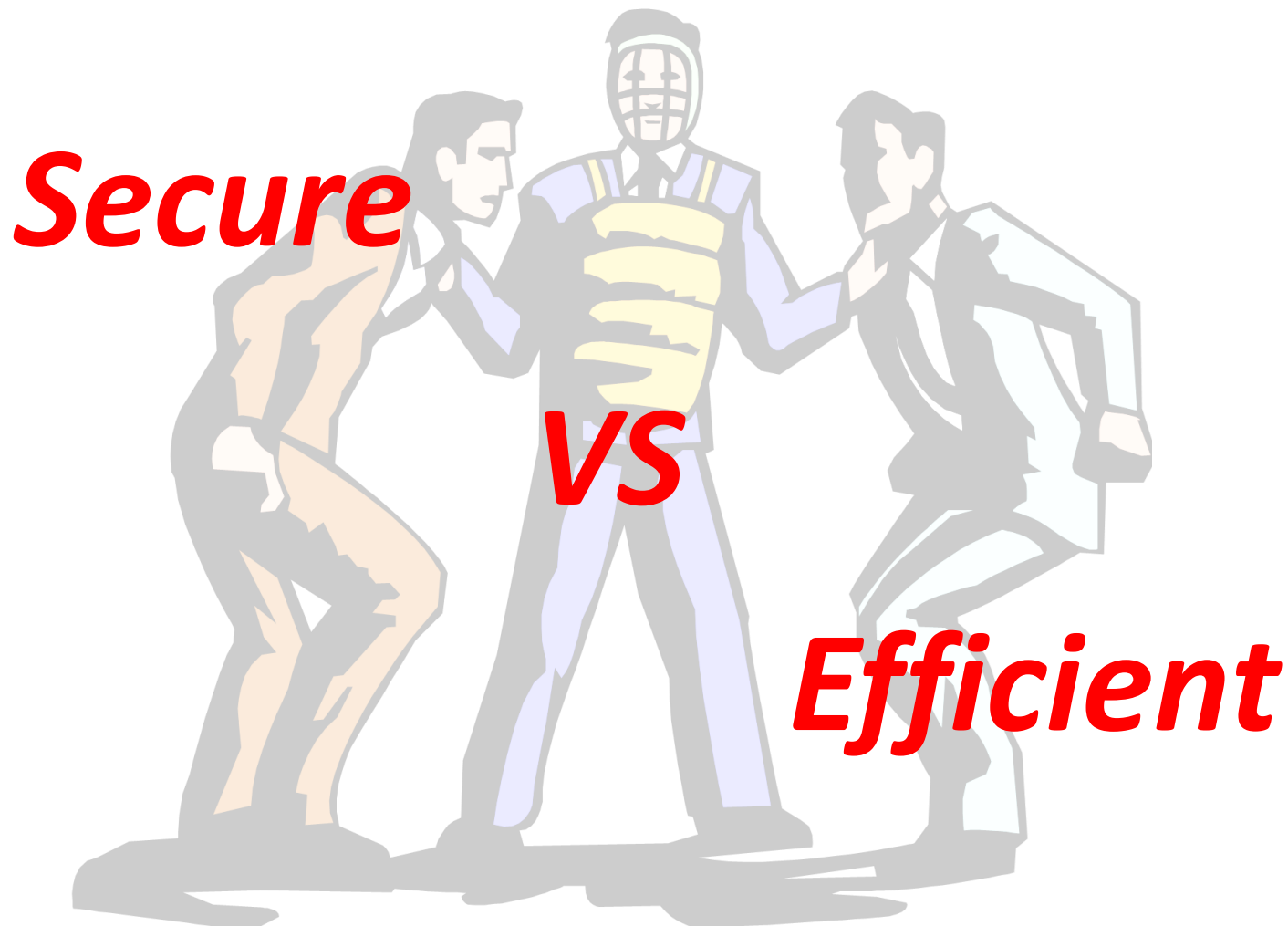
Counter (CTR) mode decryption

Format Preserving Encryption

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



Secure? Efficient?

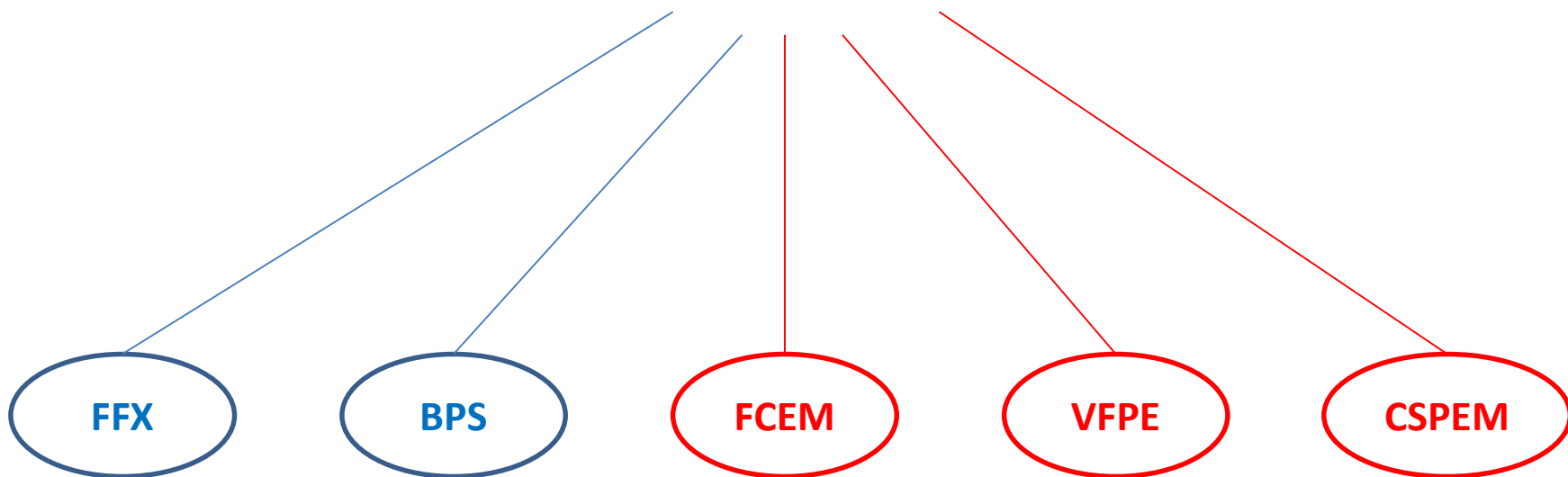


Secure? Efficient?

Efficient?

Secure?

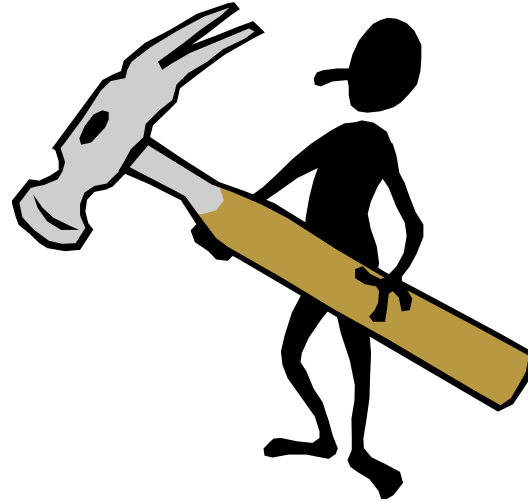
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



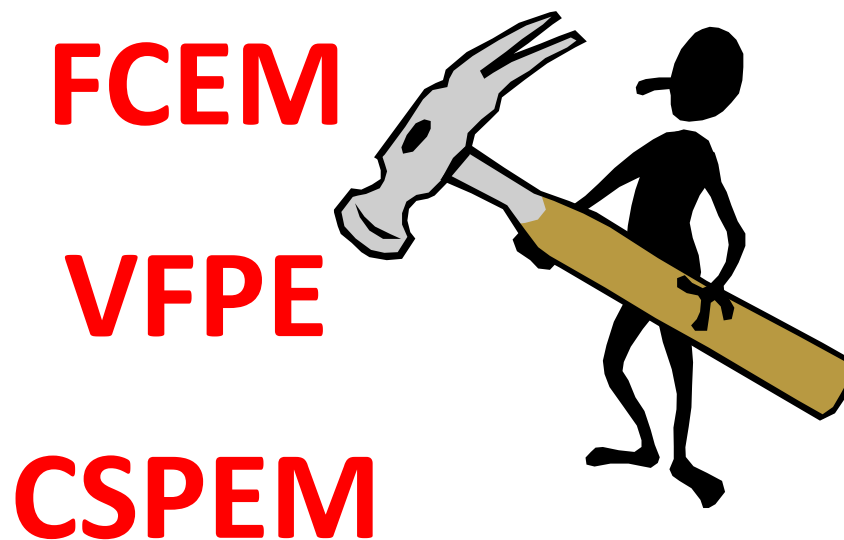
Make Efficiently

FFX

BPS



Make Securely



Thank you.



kanghc@korea.ac.kr