Practical Cryptographic Systems

Symmetric Cryptography III

Instructor: Matthew Green

Housekeeping

- A1 due tomorrow!
- Reading quiz/assignment coming next Weds!
  - Boneh/Shoup book readings
  - No I will not quiz you about statistics

Numbers stations

https://www.sigidwiki.com/wiki/Category:Numbers_Stations

http://www.numbersoddities.nl/rusmilcw.html

https://en.wikipedia.org/wiki/Lincolnshire_Poacher_(numbers_station)

News

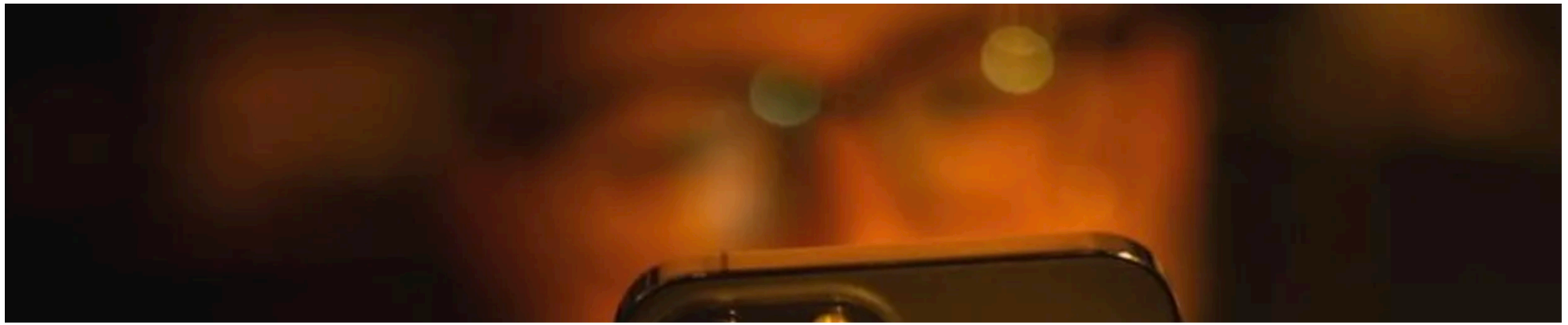
Nev

Apple says UK could 'secretly veto' global privacy tools

29th January 2024, 12:36 EST

Share

By Zoe Kleinman
Technology editor



Apple has attacked proposals for the UK government to pre-approve new security features introduced by tech firms.

Under the proposed amendments to existing laws, if the UK Home Office declined an update, it then could not be released in any other country, and the public would not be informed.

The government is seeking to update the Investigatory Powers Act (IPA) 2016.

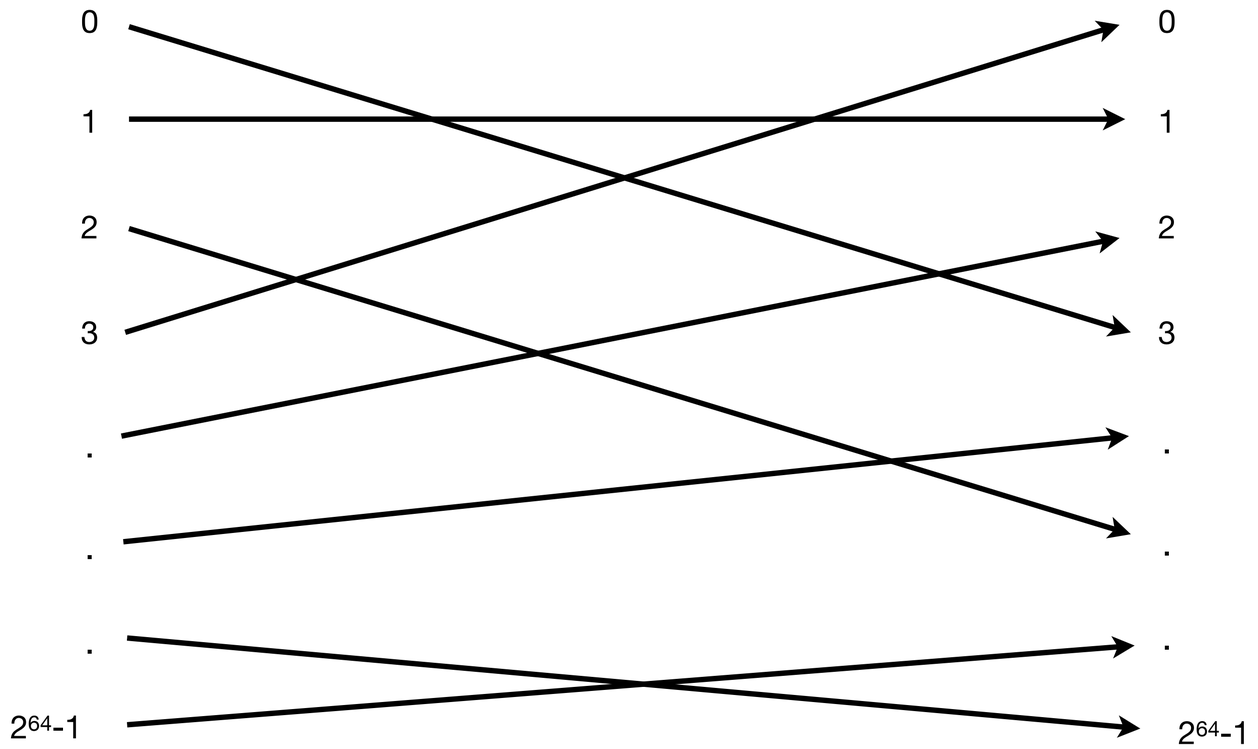
The Home Office said it supported privacy-focused tech but added that it also had to keep the country safe.

A government spokesperson said: "We have always been clear that we support technological innovation and private and secure communications technologies, including end-to-end encryption, but this cannot come at a cost to public safety."

The proposed changes will be debated in the House of Lords tomorrow.

Apple says it is an "unprecedented overreach" by the UK government.

Permutation



Ciphers / Permutation Families

- Can’t have just one permutation
  - Alice & Bob know the permutation
    Adversary should not
  - Permutation is “random” (ish)
  - For a 64-bit input block, how many possible permutations are there?

Ciphers / Permutation Families

- Can’t have just one permutation
  - Alice & Bob know the permutation
    Adversary should not
  - Permutation is “random” (ish)
  - For a 64-bit input block, how many possible permutations are there?
  - How does this compare to DES key length?

Block Cipher

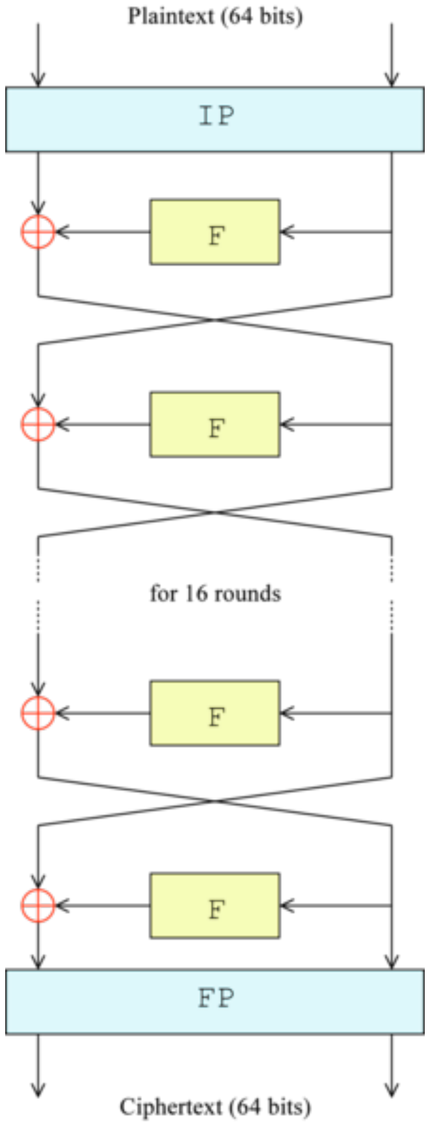
- Block cipher is a family of permutations
  - Indexed by a key (DES = 56 bit key)
  - “Pseudo-random”

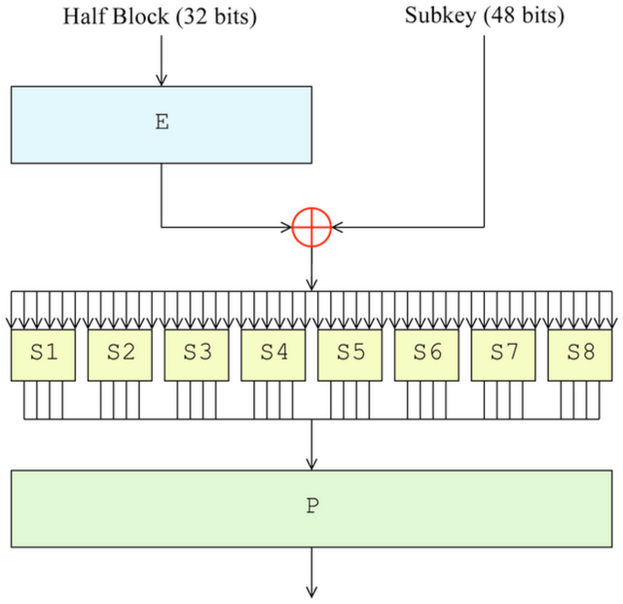
Block Cipher

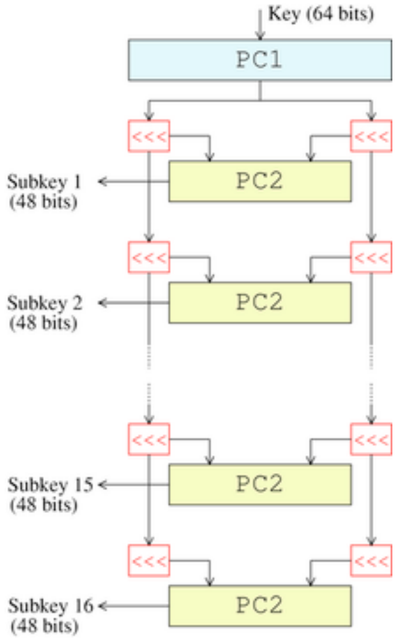
- Block cipher is a family of permutations
  - Indexed by a key (DES = 56 bit key)
  - Ideally: “Pseudo-random permutation (PRP)”

    (i.e., attacker who does not know the key can’t determine whether you’re using a random permutation, or a PRP)

DES: 64-bit Block, 56-bit Key

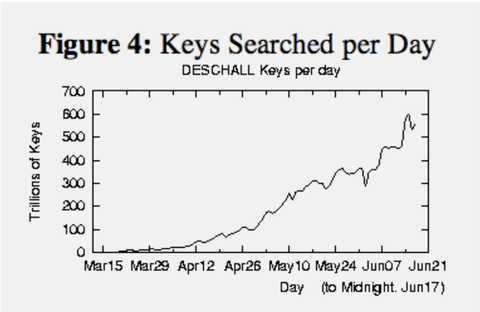


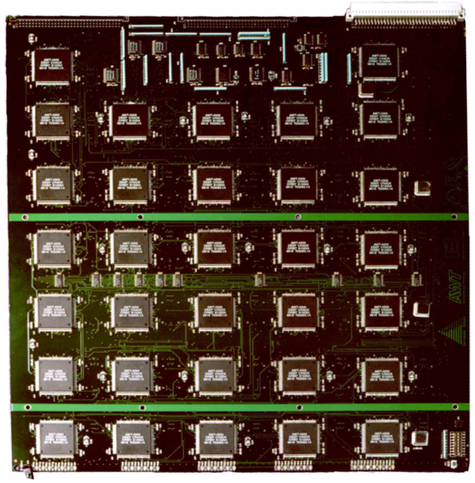




DES

- Some “clever” attacks on DES
  - However: practical weakness = 56 bit key size
  - Practical solution: 3DES (also deprecated)





U.S. Data-Scrambling Code Cracked With Homemade Equipment

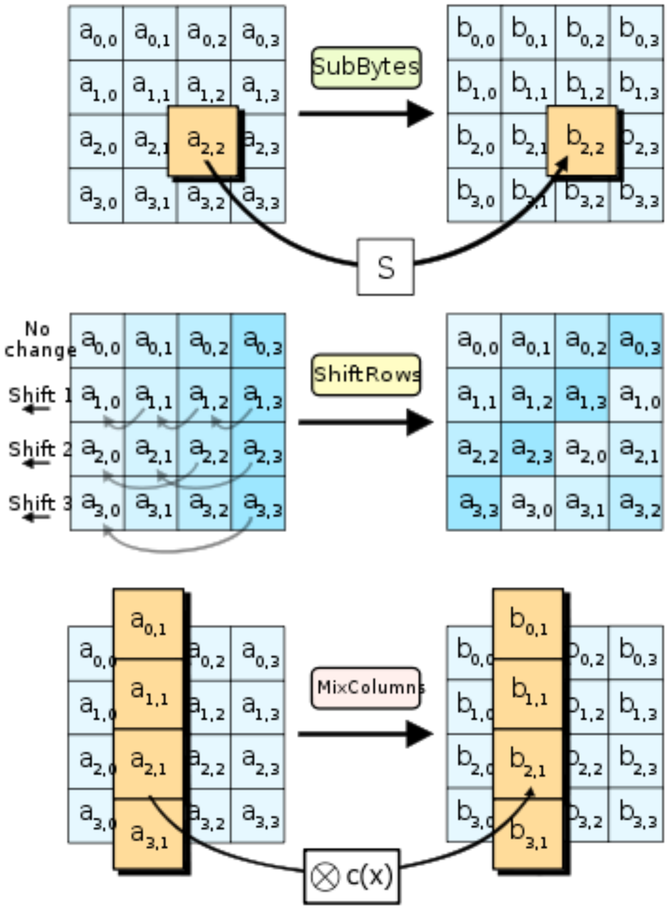
By JOHN MARKOFF

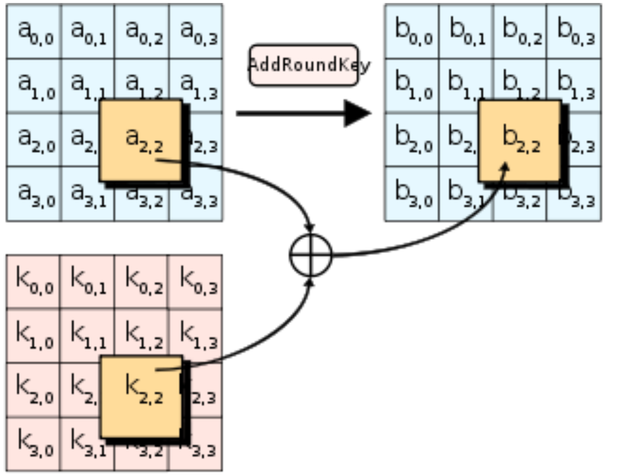
SAN FRANCISCO -- In a 1990s variant of a John Henry-style competition between man and machine, researchers using a homemade supercomputer have cracked the government's standard data-scrambling code in record time -- and have done it by out-calculating a team that had harnessed thousands of computers, including some of the world's most powerful.

AES

- NIST open competition (around 1998). Requirements:
  - Fast in software & hardware
  - Larger block size (128 bit)
  - Longer keys (128/192/256-bit)
  - Reviewed by academics & NSA
- 5 finalists:
  - MARS, RC6, Rijndael, Serpent, and Twofish

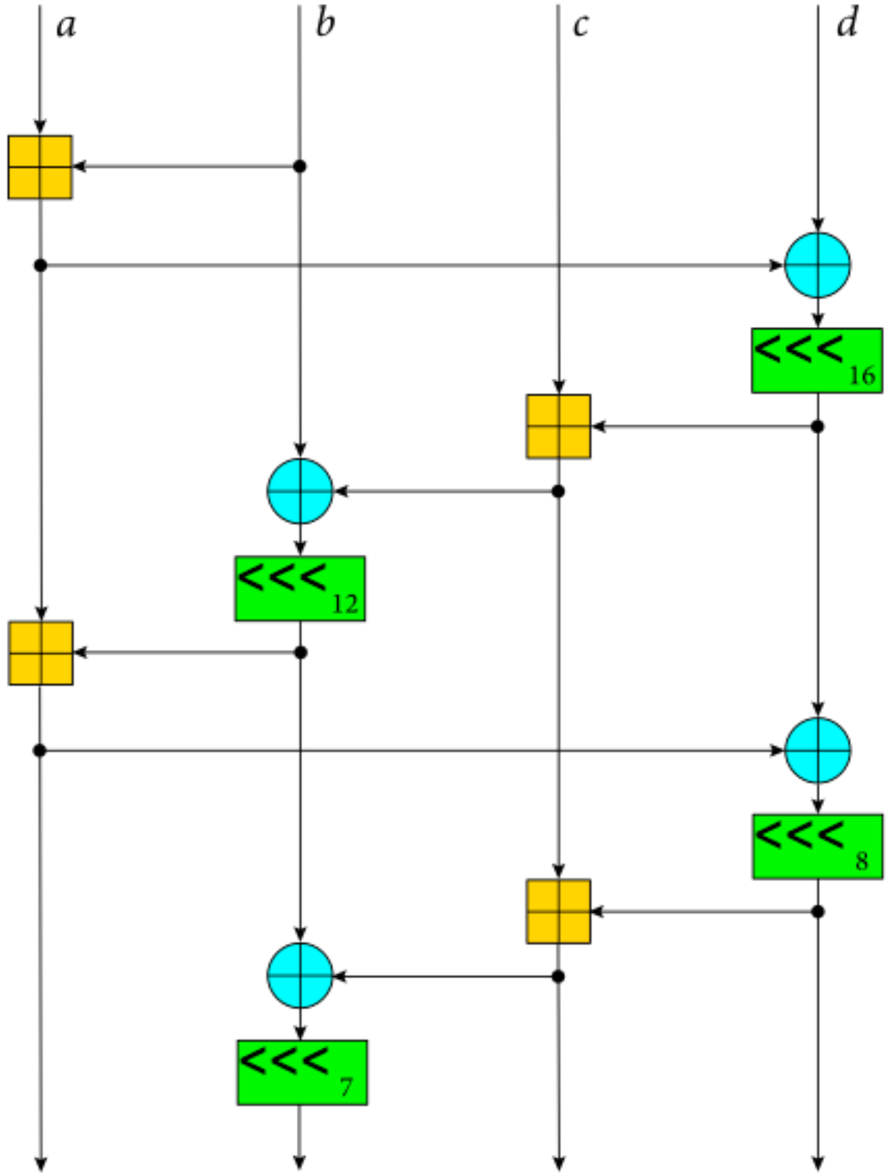
AES: 128-bit Block, 128/192/256-bit Key





ChaCha20

(Not a block cipher!)



Using Block Ciphers

- ECB is not semantically secure, hence we use a “mode of operation”
  - e.g., CBC, CTR, CFB, OFB (and others)
- These provide:
  - Security for multi-block messages
  - Randomization (through an Initialization Vector)

Using Block Ciphers

- Obvious (bad) idea:
  - Take every consecutive chunk of plaintext
  - Pass it into the block cipher
  - Concatenate all the output blocks
  - This is called “Electronic Codebook Mode” (ECB)

Using Block Ciphers

- Obvious (bad) idea:
  - Take every consecutive chunk of plaintext
  - Pass it into the block cipher
  - Concatenate all the output blocks
  - This is called “Electronic Codebook Mode” (ECB)
- **What’s the problem with this?**

ECB Mode

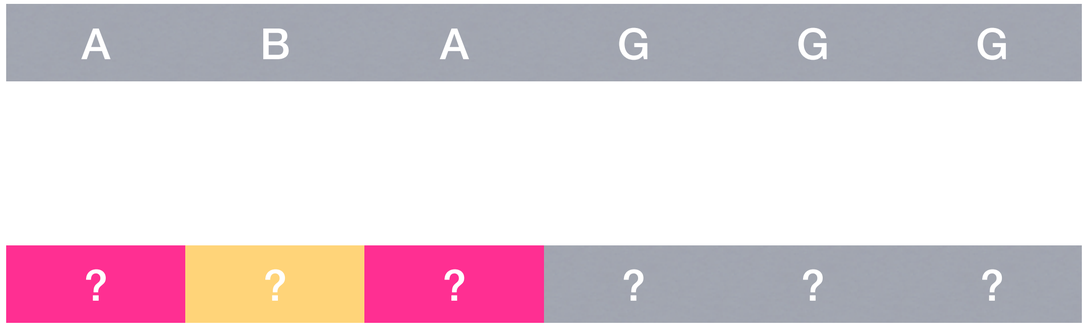
- Problem #1: ECB is deterministic

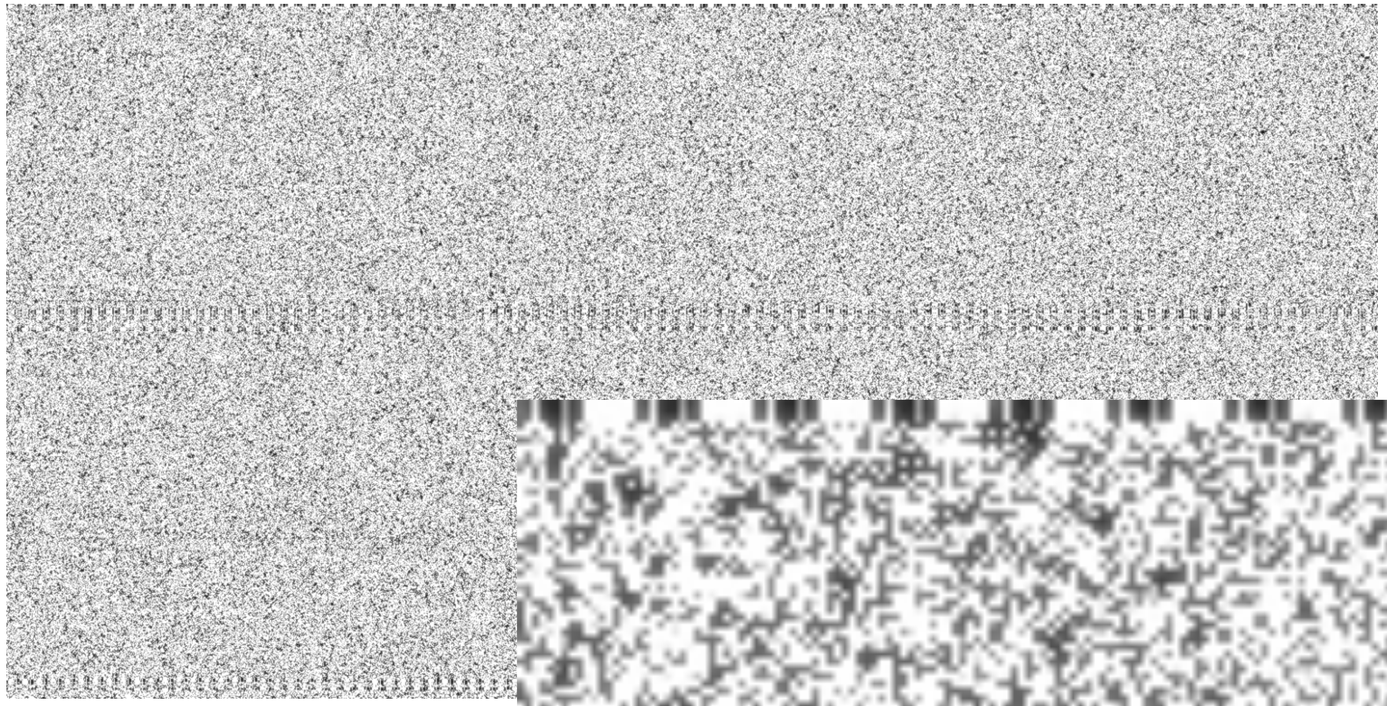
E(Attack Monster)

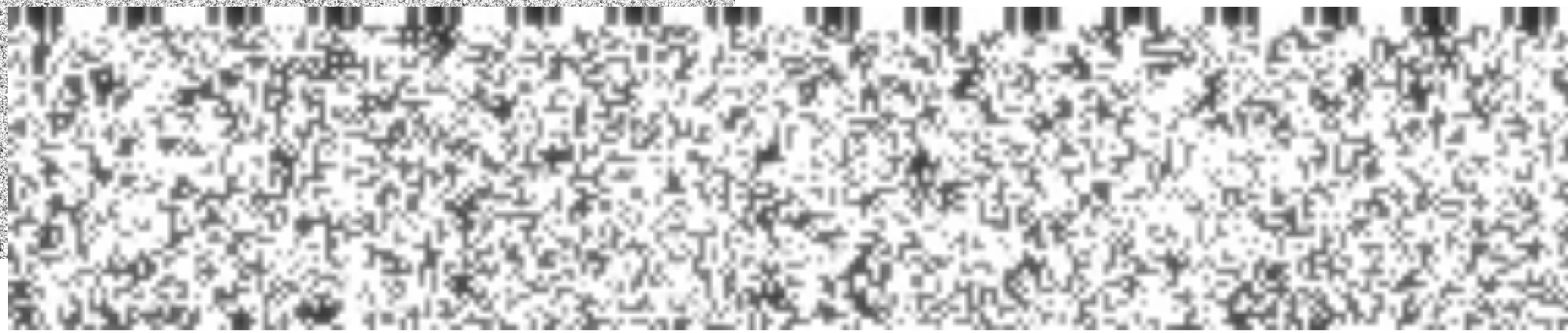
E(Monster Attacks)

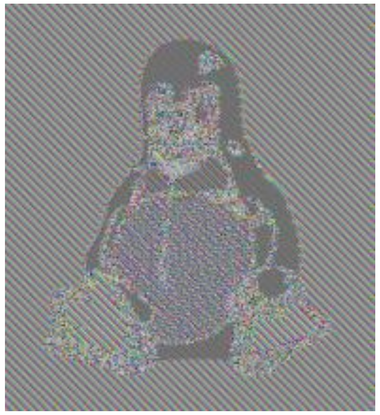
ECB Mode

- Problem #2: Leakage of plaintext patterns









Security of Encryption

- Semantic Security
  - Due to Goldwasser & Micali (1980s)
  - Informally: An encryption scheme is secure if adversary who sees ciphertext “learns as much” as adversary who doesn’t see ciphertext.

•Even if adversary can request chosen plaintexts

  - How do we state this formally?

Semantic security

- Semantic Security (IND-CPA)

$M_1, ..., M_n$

$E(k, M_1), ..., E(k, M_n)$

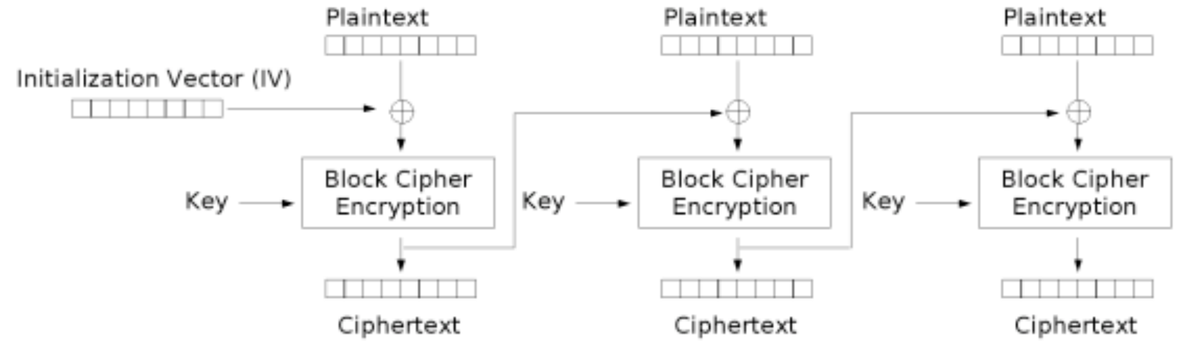
M_0, M_1

$E(M_b)$

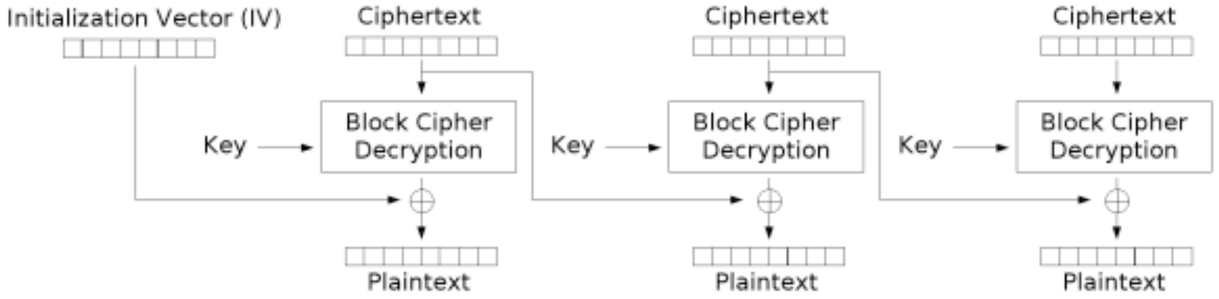
Using Block Ciphers

- ECB is not semantically secure, hence we use a “mode of operation”
  - e.g., CBC, CTR, CFB, OFB (and others)
- These provide:
  - Security for multi-block messages
  - Randomization (through an Initialization Vector)

CBC Mode



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Security of CBC

- Is CBC a secure encryption scheme?
  - Yes, assuming a secure block cipher (and a passive adversary)
  - Correct (random) IV generation
  - Can prove this under assumption that
    block cipher = Pseudo-Random Permutation (PRP)
- Bellare, Desai, Jokipii & Rogaway (2000)
  - Easy to use wrong...
    - Most important: use a unique & random IV!

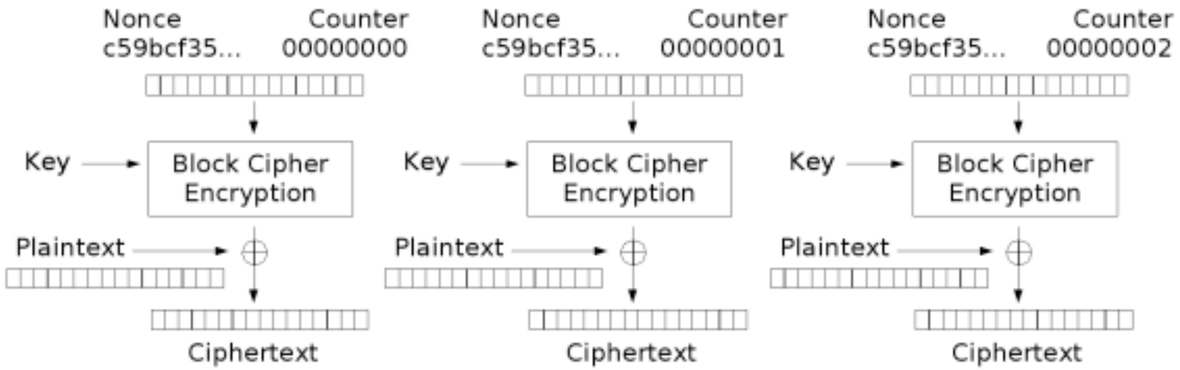
The size of the frame of data to be encrypted or decrypted (i.e. how often a new CBC chain is started) depends on the particular application, and is defined for each in the corresponding format specific books of this specification. Unless otherwise specified, the Initialization Vector used at the beginning of a CBC encryption or decryption chain is a constant, $iv_{0,}$ which is:

$0BA0F8DDFEA61FB3D8DF9F566A050F78_{16}$

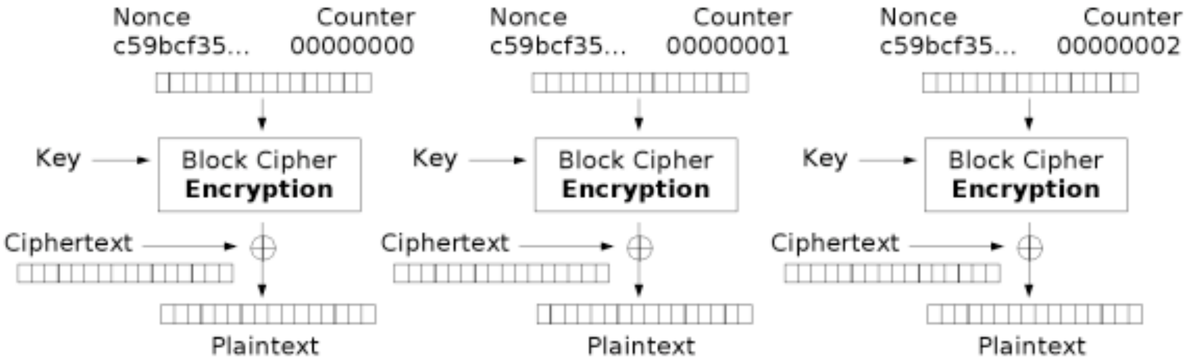
Advanced Access Content System (AACS)

Introduction and Common Cryptographic Elements

CTR Mode



Counter (CTR) mode encryption



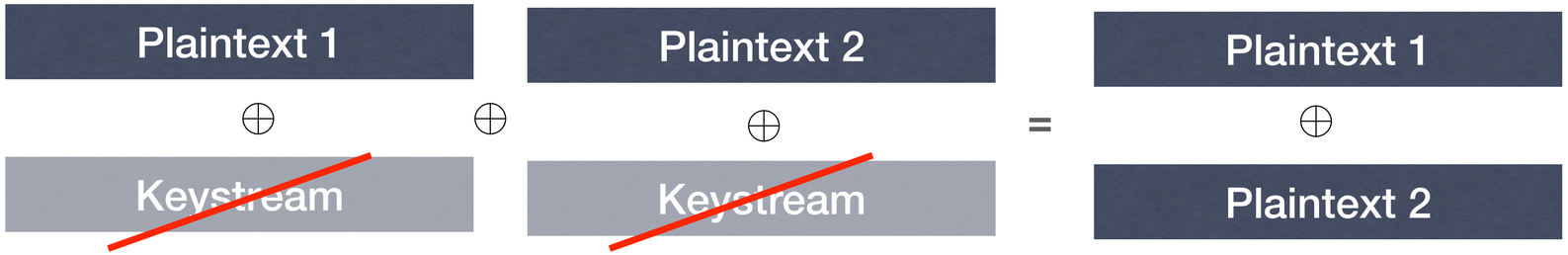
Counter (CTR) mode decryption

CTR (intuition)

- CTR uses the cipher to expand a short cipher key (K) into a long string of pseudorandom output bits
  - This is called a “**keystream**”
  - We then XOR the keystream with a long message (or many messages)
  - This turns a block cipher into a “stream cipher”

Security of CTR

- Yes, assuming secure block cipher (PRP)
- However, counter range must never be re-used



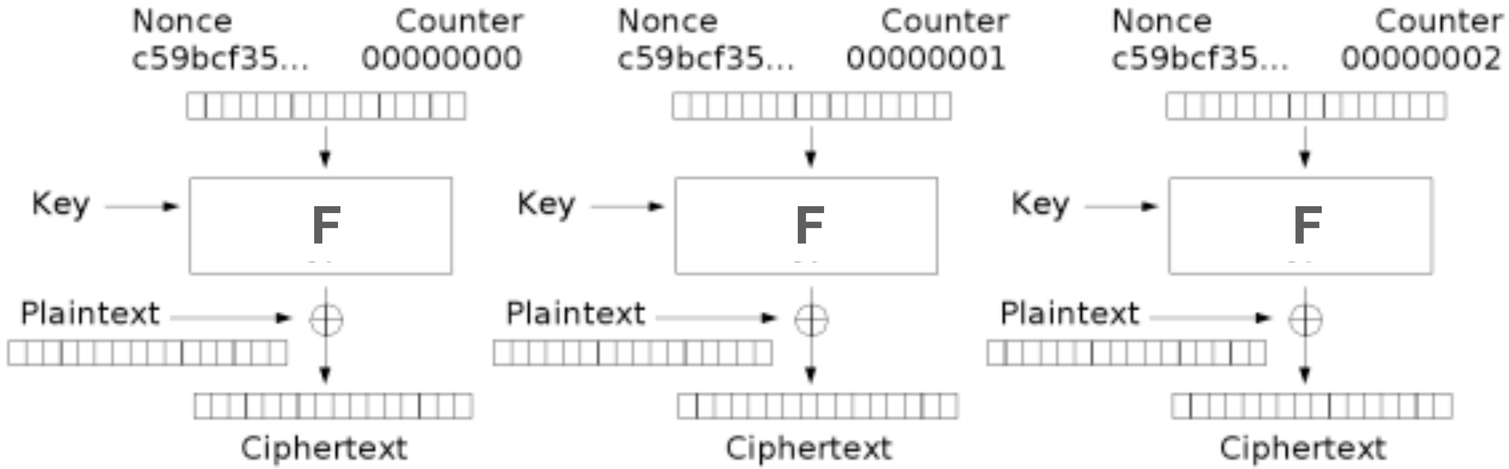
- Similar example: MS Word 2003
  - (they used RC4, but same problem)

CTR with other functions

- We've been assuming a cipher that is invertible (a permutation/block cipher)
- **Observation:** CTR never uses the "Decipher" (invert) algorithm of the cipher
  - So what if we don't use a block cipher at all?

CTR with other functions

- We've been assuming a cipher that is invertible (a permutation/block cipher)
- **Observation:** CTR never uses the "Decipher" (invert) algorithm of the cipher
  - So what if we don't use a block cipher at all?



Counter (CTR) mode encryption