CSE 484 / CSE M 584: Computer Security and Privacy

Cryptography

Autumn 2018

Tadayoshi (Yoshi) Kohno
yoshi@cs.Washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Ada Lerner, John Manferdelli, John Mitchell, Franziska Roesner, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Admin

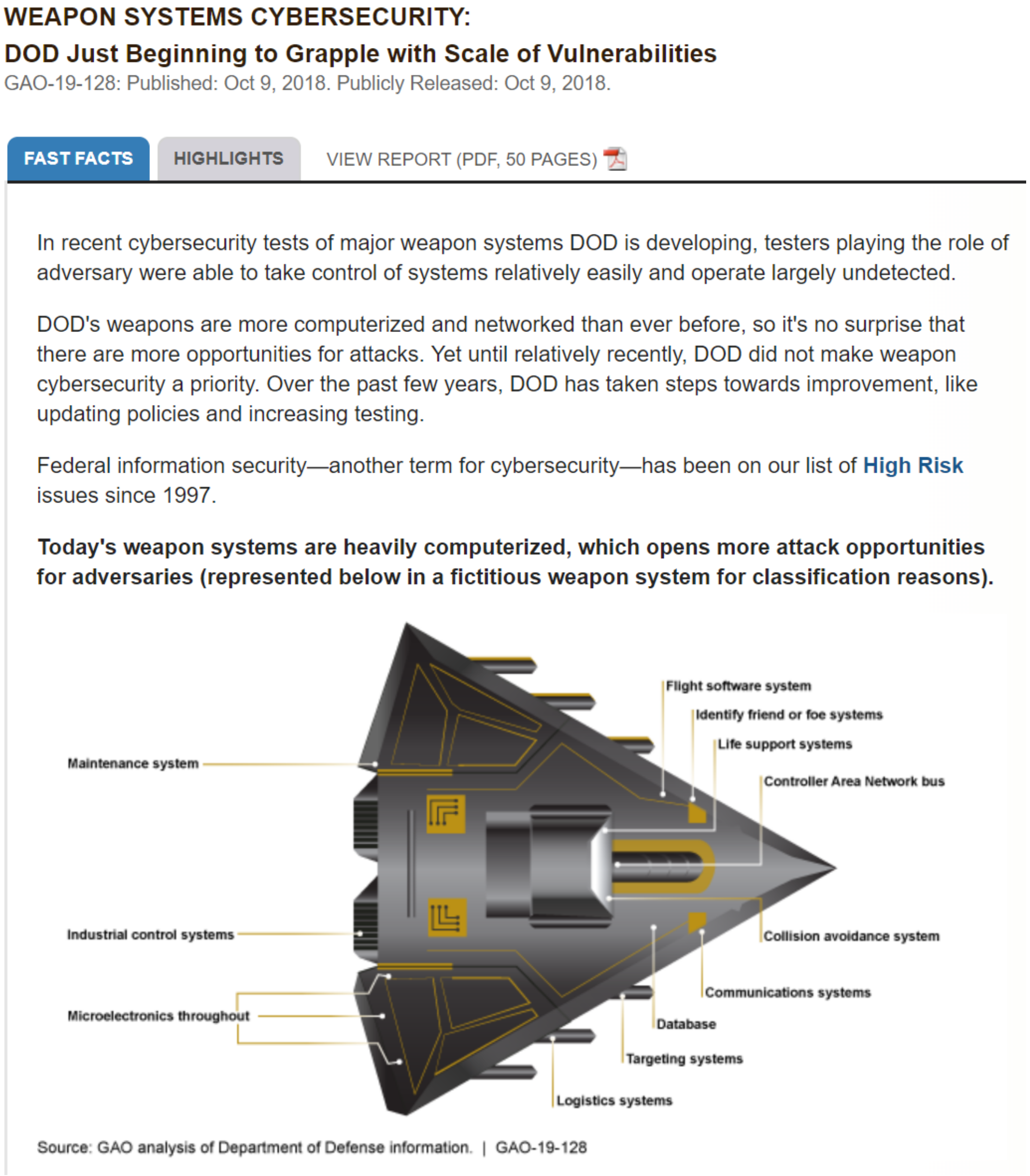
- Lab 1:
  - Due Oct 24, 4:30pm

- Quiz sections (especially for Lab 1): M 2:30, W 1:30, F 12
- My office hours (especially for crypto, research readings, administrivia, worksheet pick up): M 11:30

- Questions about David Aucsmith's talk?

Some Notes on David Aucsmith's Talk

- Cyber Crime
- Cyber Espionage
- Cyber Warfare



WEAPON SYSTEMS CYBERSECURITY:

DOD Just Beginning to Grapple with Scale of Vulnerabilities

GAO-19-128: Published: Oct 9, 2018. Publicly Released: Oct 9, 2018.

In recent cybersecurity tests of major weapon systems DOD is developing, testers playing the role of adversary were able to take control of systems relatively easily and operate largely undetected.

DOD's weapons are more computerized and networked than ever before, so it's no surprise that there are more opportunities for attacks. Yet until relatively recently, DOD did not make weapon cybersecurity a priority. Over the past few years, DOD has taken steps towards improvement, like updating policies and increasing testing.

Federal information security—another term for cybersecurity—has been on our list of **High Risk** issues since 1997.

Today's weapon systems are heavily computerized, which opens more attack opportunities for adversaries (represented below in a fictitious weapon system for classification reasons).

Flight software system
Identify friend or foe systems
Life support systems
Maintenance system
Controller Area Network bus
Industrial control systems
Collision avoidance system
Communications systems
Microelectronics throughout
Database
Targeting systems
Logistics systems

Source: GAO analysis of Department of Defense information. | GAO-19-128

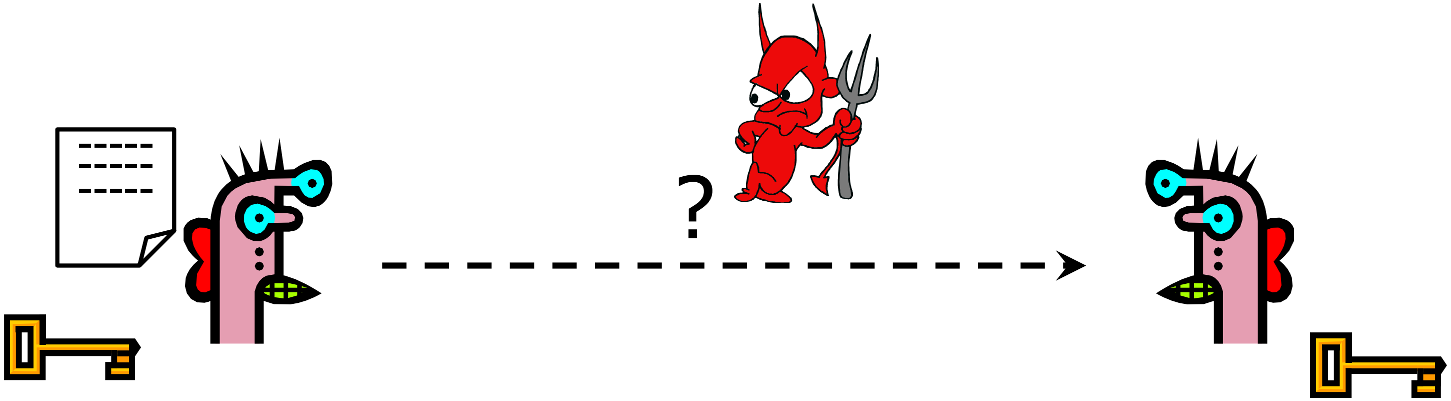
https://www.gao.gov/products/GAO-19-128

Review Slides (Overview)

Flavors of Cryptography

- Symmetric cryptography
  - Both communicating parties have access to a shared random string K, called the key.
  - Challenge: How do you privately share a key?
- Asymmetric cryptography
  - Each party creates a public key pk and a secret key sk.
  - Challenge: How do you validate a public key?

Confidentiality: Basic Problem



Given (Symmetric Crypto): both parties know the same secret.

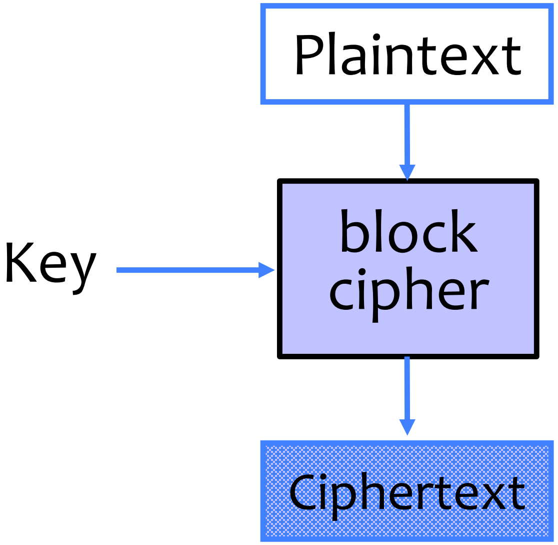
Goal: send a message confidentially.

Ignore for now: How is this achieved in practice??

Review Slides (Block Ciphers)

Block Ciphers

- Operates on a single chunk (“block”) of plaintext
  - For example, 64 bits for DES, 128 bits for AES
  - Each key defines a different permutation
  - Same key is reused for each block (can use short keys)



Standard Block Ciphers

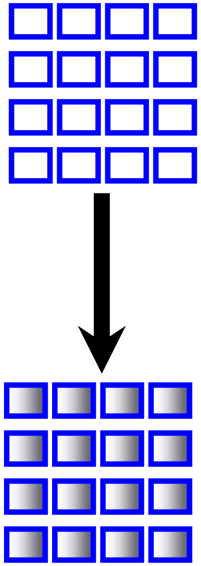
- **DES: Data Encryption Standard**
  - Feistel structure: builds invertible function using non-invertible ones
  - Invented by IBM, issued as federal standard in 1977
  - 64-bit blocks, 56-bit key + 8 bits for parity

- **AES: Advanced Encryption Standard**
  - New federal standard as of 2001
    - NIST: National Institute of Standards & Technology
  - Based on the Rijndael algorithm
    - Selected via an open process
  - 128-bit blocks, keys can be 128, 192 or 256 bits

New Slides: How to Use Block Ciphers

Encrypting a Large Message

- So, we’ve got a good block cipher, but our plaintext is larger than 128-bit block size



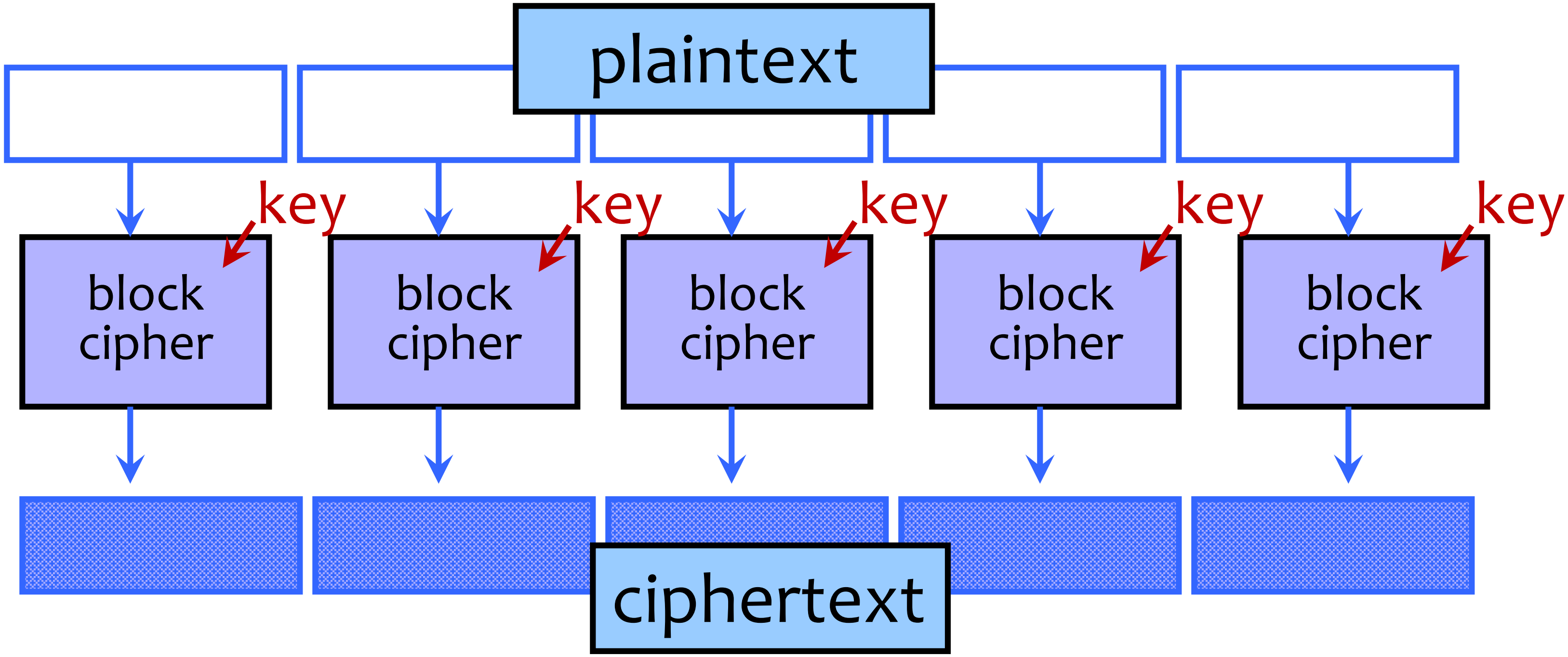
128-bit plaintext

(arranged as 4x4 array of 8-bit bytes)

128-bit ciphertext

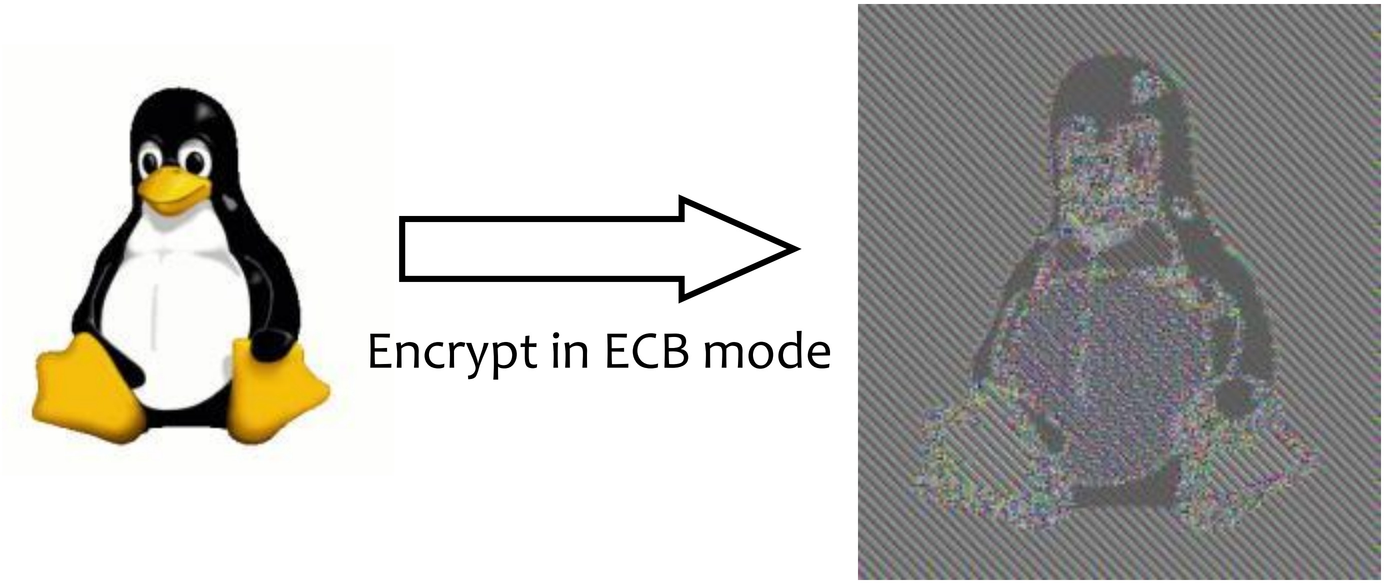
- What should we do?

Electronic Code Book (ECB) Mode



- Identical blocks of plaintext produce identical blocks of ciphertext
- No integrity checks: can mix and match blocks

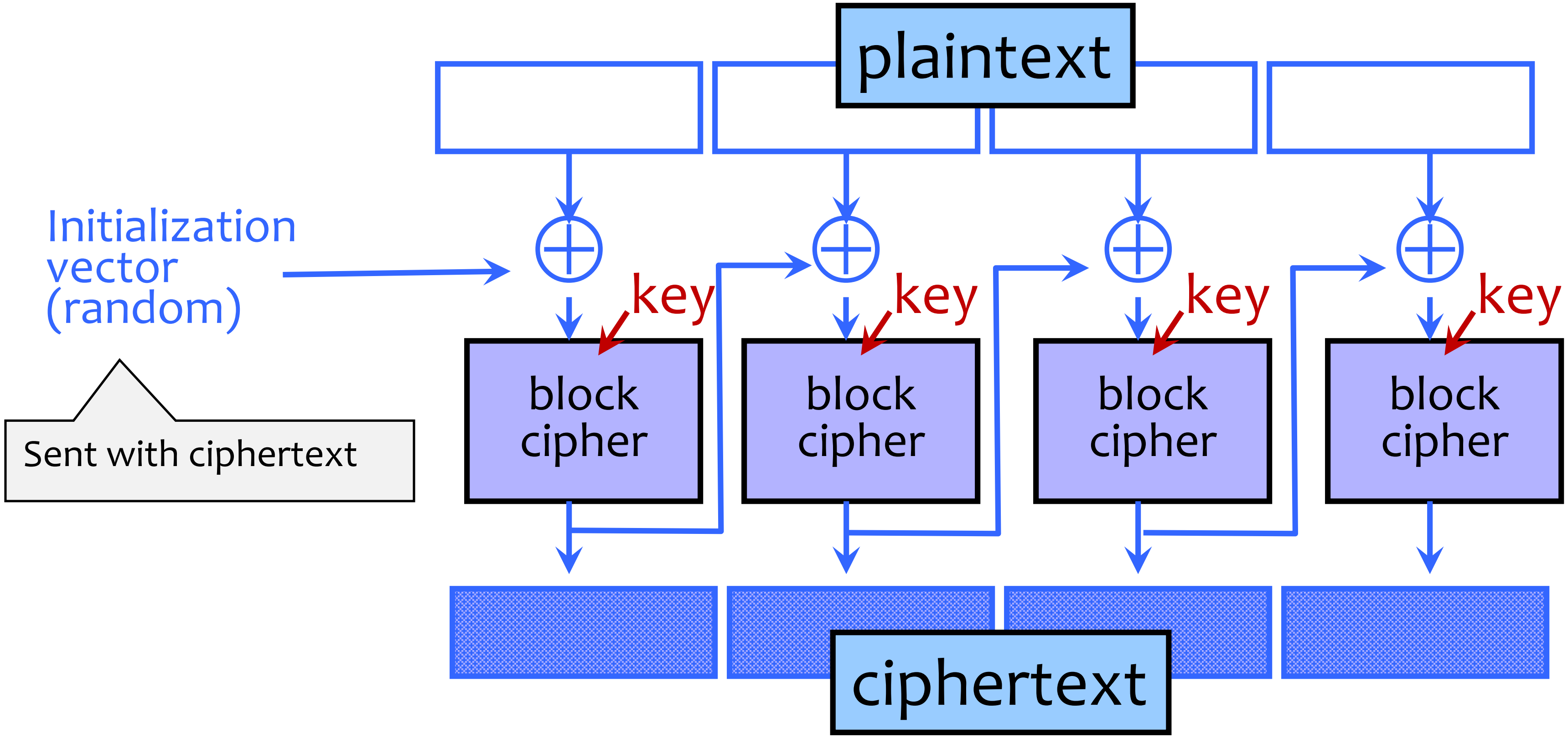
Information Leakage in ECB Mode



Encrypt in ECB mode

[Wikipedia]

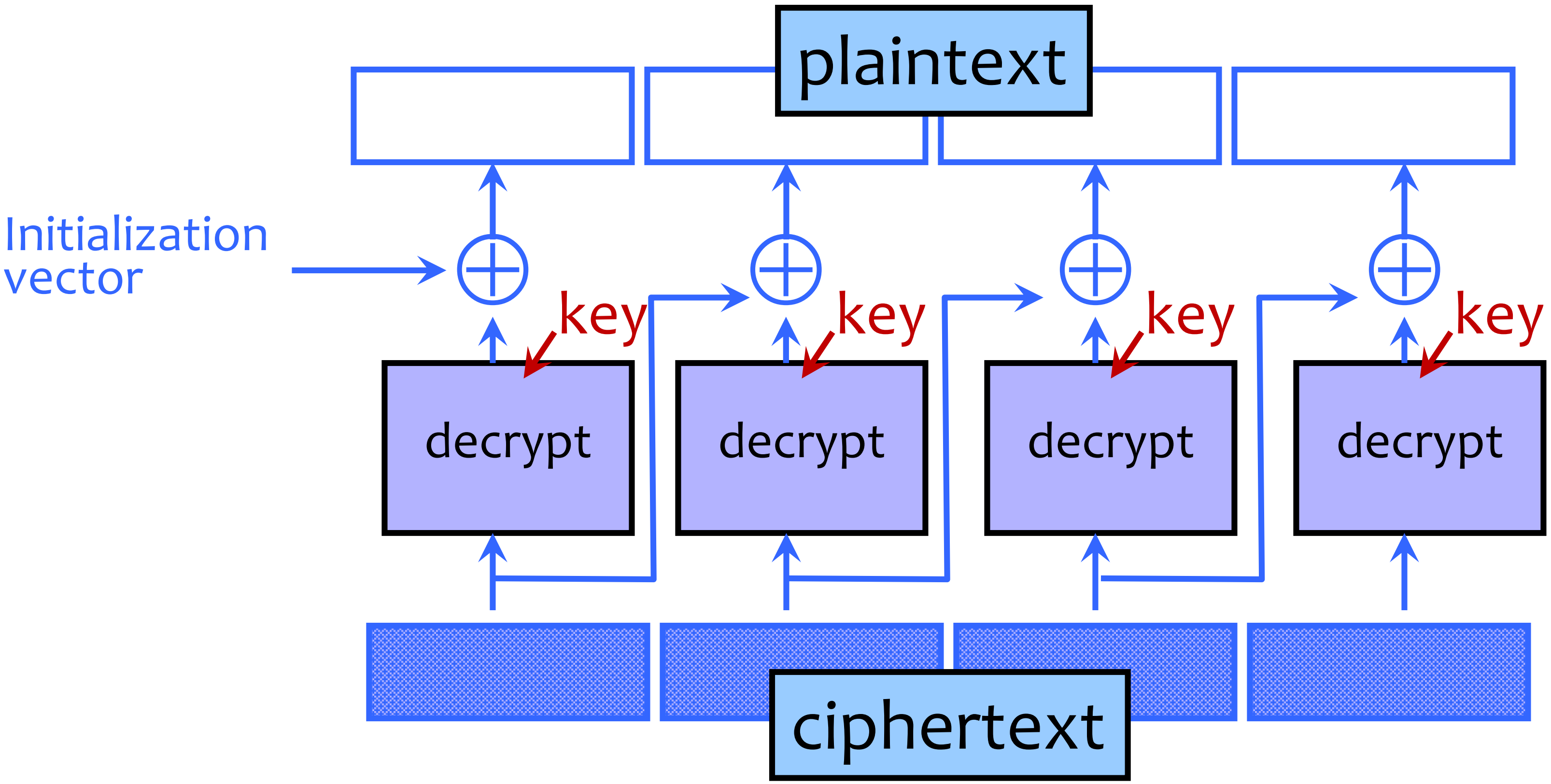
Cipher Block Chaining (CBC) Mode: Encryption



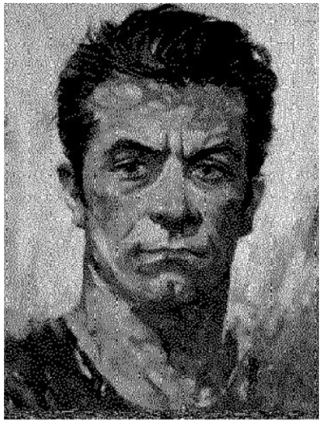
Sent with ciphertext

- Identical blocks of plaintext encrypted differently
- Last cipherblock depends on entire plaintext
  - Still does not guarantee integrity

CBC Mode: Decryption

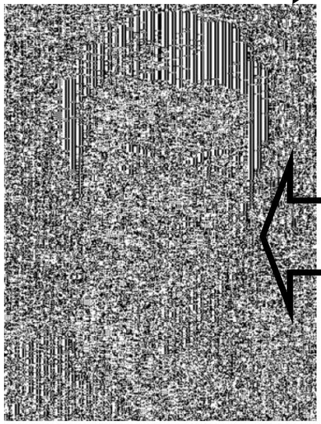


ECB vs. CBC

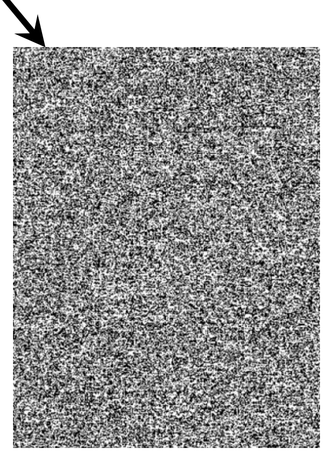


AES in ECB mode

AES in CBC mode

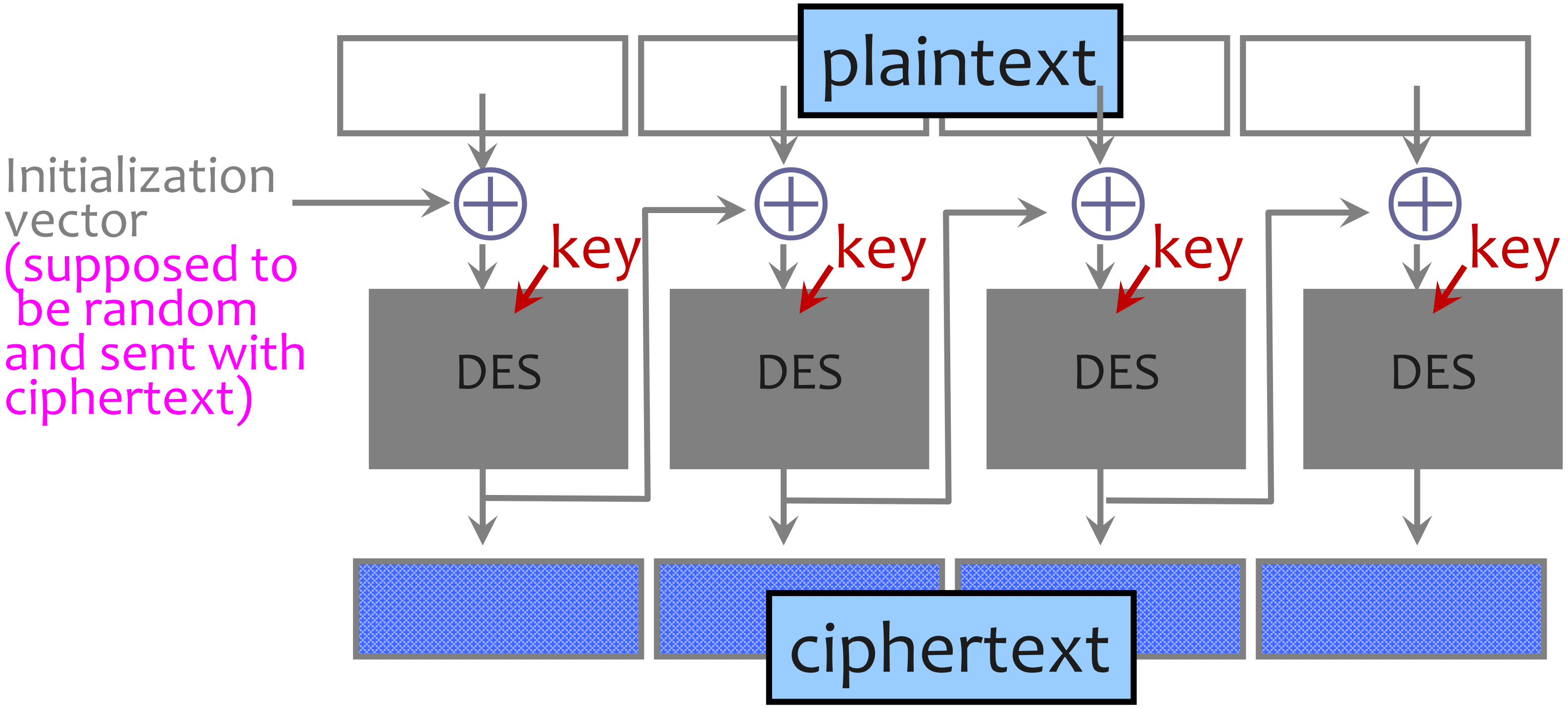


Similar plaintext blocks produce similar ciphertext blocks (not good!)



[Picture due to Bart Preneel]

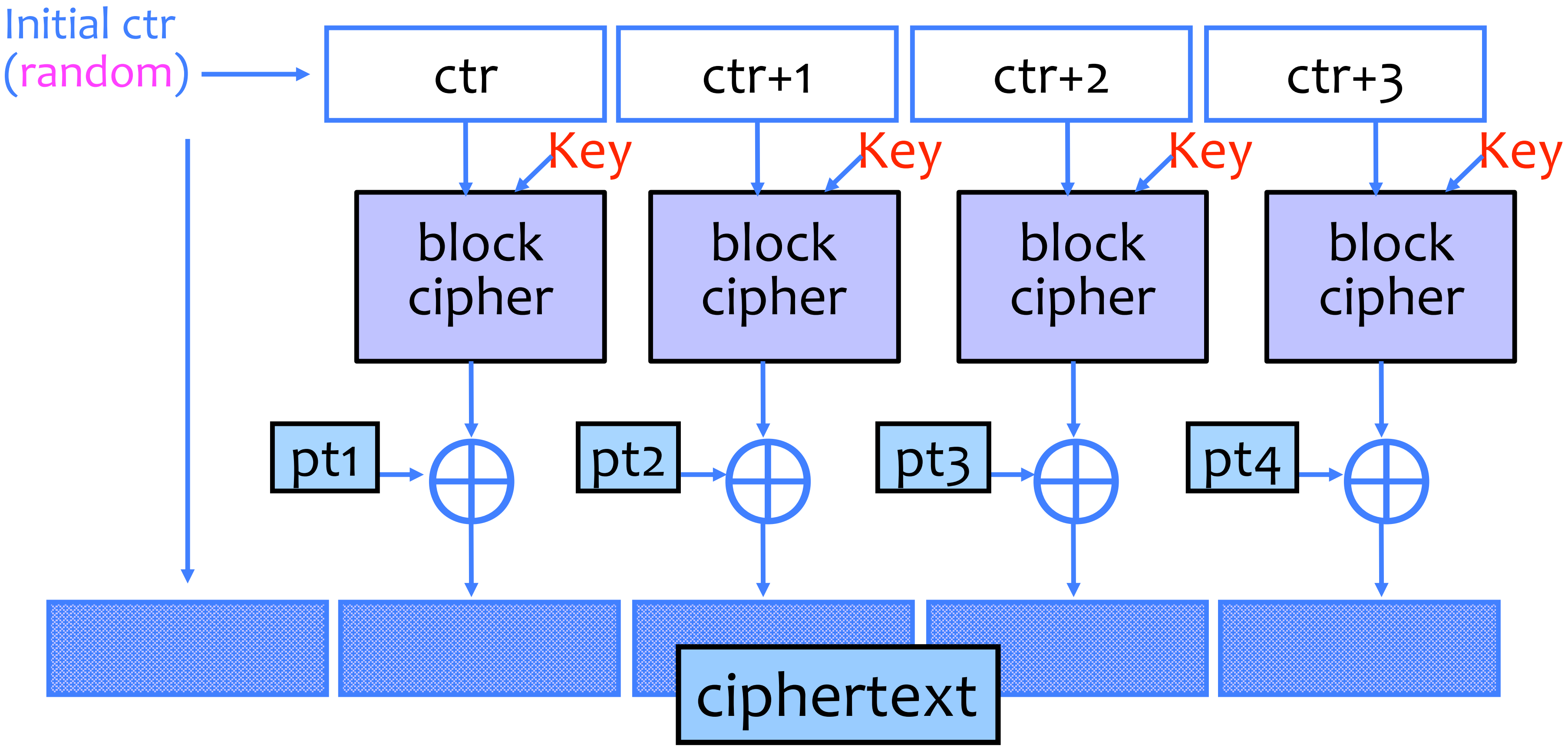
CBC and Electronic Voting



Found in the source code for Diebold voting machines:

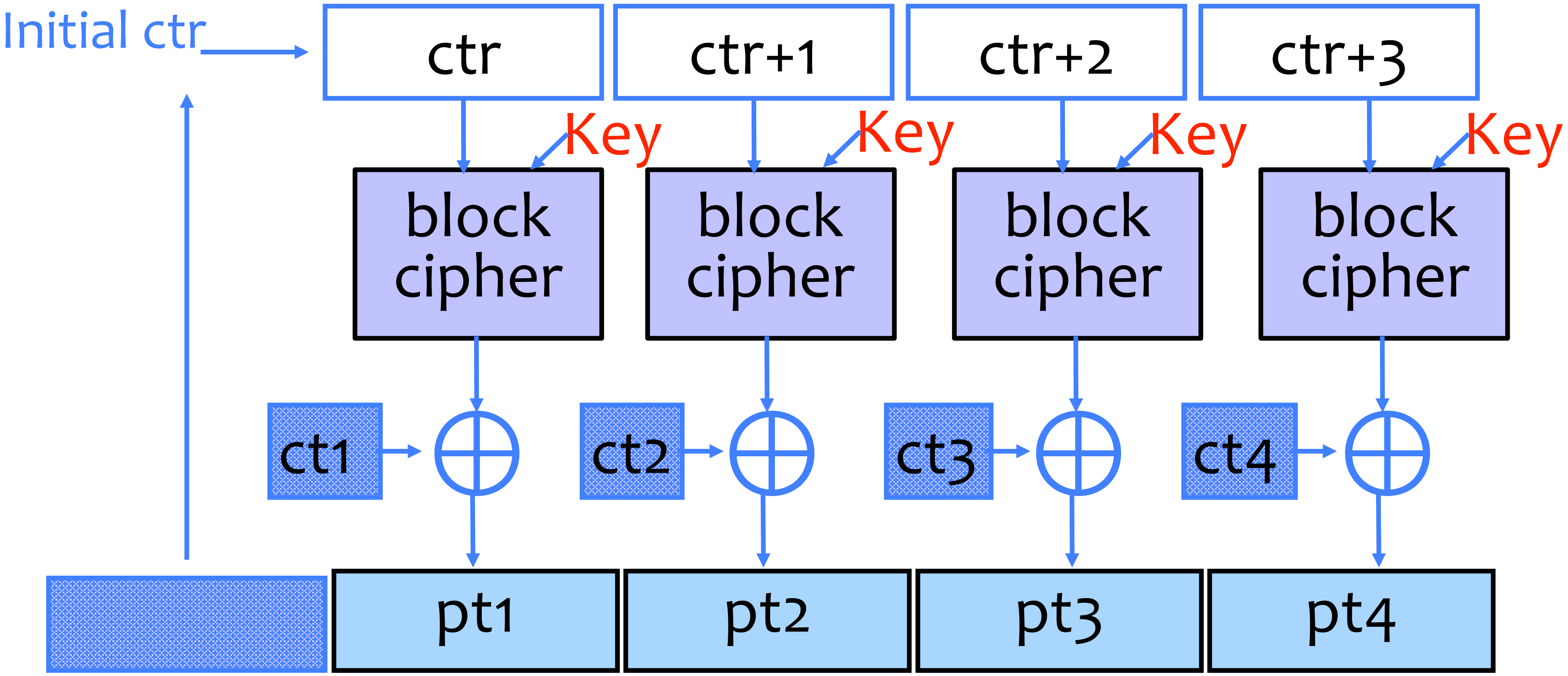
```
DesCBCEncrypt((des_c_block*)tmp, (des_c_block*)record.m_Data,
              totalSize, DESKEY, NULL, DES_ENCRYPT)
```

Counter Mode (CTR): Encryption



- Identical blocks of plaintext encrypted differently
- Still does not guarantee integrity; Fragile if ctr repeats

Counter Mode (CTR): Decryption



Flavors of Cryptography

- Symmetric cryptography
  - Both communicating parties have access to a shared random string K, called the key.
  - Challenge: How do you privately share a key?
- Asymmetric cryptography
  - Each party creates a public key pk and a secret key sk.
  - Challenge: How do you validate a public key?

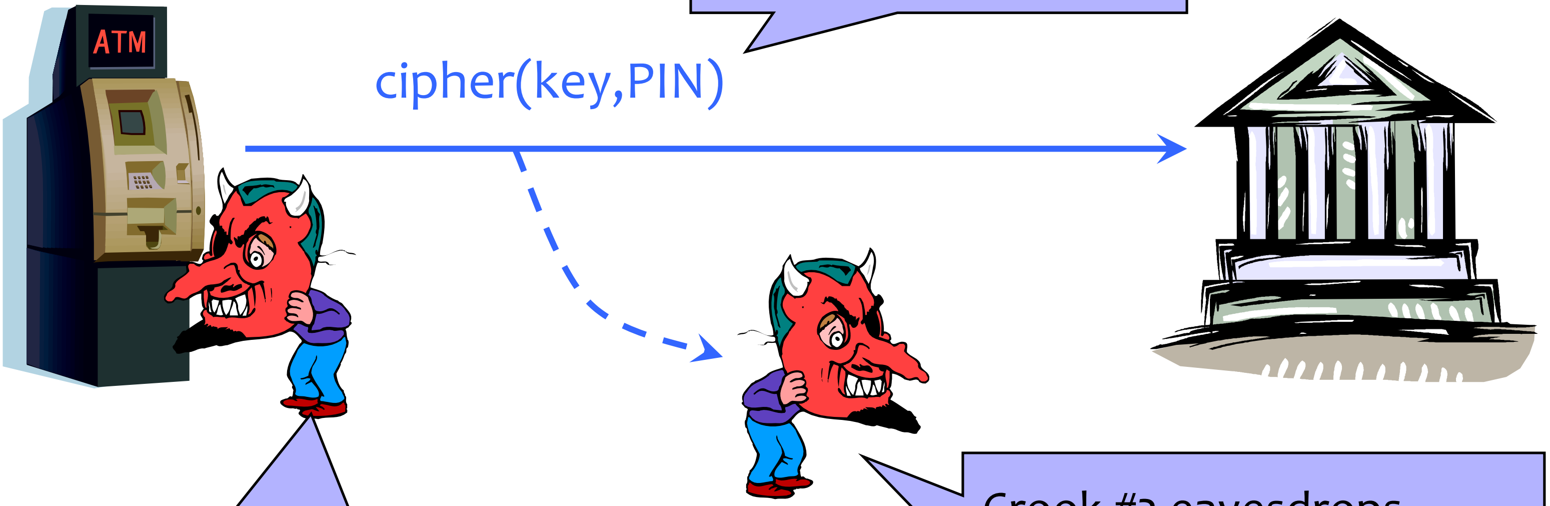
When is an Encryption Scheme “Secure”?

- Hard to recover the key?
  - What if attacker can learn plaintext without learning the key?
- Hard to recover plaintext from ciphertext?
  - What if attacker learns some bits or some function of bits?

How Can a Cipher Be Attacked?

- Attackers knows ciphertext and encryption algthm
  - What else does the attacker know? Depends on the application in which the cipher is used!
- Ciphertext-only attack
- KPA: Known-plaintext attack (stronger)
  - Knows some plaintext-ciphertext pairs
- CPA: Chosen-plaintext attack (even stronger)
  - Can obtain ciphertext for any plaintext of their choice
- CCA: Chosen-ciphertext attack (very strong)
  - Can decrypt any ciphertext except the target

Chosen Plaintext Attack



PIN is encrypted and transmitted to bank

cipher(key,PIN)

Crook #1 changes their PIN to a number of their choice

Crook #2 eavesdrops on the wire and learns ciphertext corresponding to chosen plaintext PIN

… repeat for any PIN value

Very Informal Intuition

Minimum security requirement for a modern encryption scheme

- Security against chosen-plaintext attack (CPA)
  - Ciphertext leaks no information about the plaintext
  - Even if the attacker correctly guesses the plaintext, they cannot verify their guess
  - Every ciphertext is unique, encrypting same message twice produces completely different ciphertexts
    - Implication: encryption must be randomized or stateful
- Security against chosen-ciphertext attack (CCA)
  - Integrity protection – it is not possible to change the plaintext by modifying the ciphertext