Computer Security (COM-301)

Applied cryptography I

Interactive Exercises

ECB properties

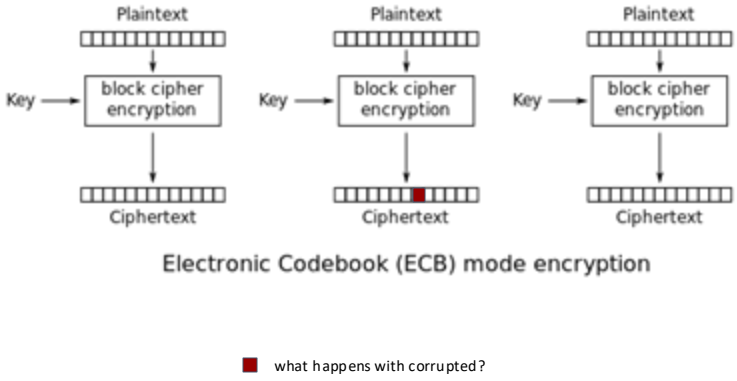
To encrypt a series of plaintext blocks p1, p2, . . . pn using a block cipher E operating in electronic code book (ECB) mode, each ciphertext block c1, c2, . . . cn is computed as ci = Ek(pi).

Which of the following is **not** a property of this block cipher mode?

a) Any repeated plaintext blocks will result in identical corresponding ciphertext blocks.
b) Decryption can be fully parallelized.
c) If a ciphertext block is modified or corrupted, then after decryption the corresponding plaintext block and all the following plaintext blocks will be affected.
d) None of the above; that is, (a), (b), and (c) are all properties of the ECB block cipher mode.

The correct answer is (c). In ECB, altering a ciphertext block only affects a single plaintext block, see diagram after with the red marker.
(a) and (b) are in the slides

ECB properties



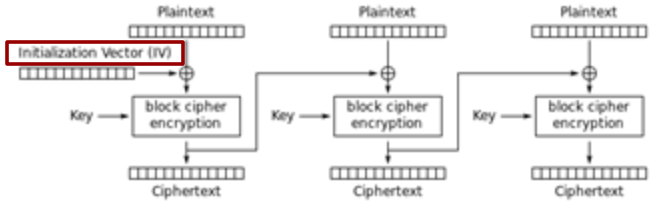
when decrypting, only the plaintext block above is affected

Randomness matters

Why use a random IV in CBC (cipher block chaining) mode encryption?
What goes wrong if one uses a fixed IV?

Randomness matters

Why use a random IV in CBC (cipher block chaining) mode encryption? What goes wrong if one uses a fixed IV?



Cipher Block Chaining (CBC) mode encryption

If the IV is not changed and if the two messages share the first block, the input to the first encryption block would be the same: identical plaintexts would be encrypted to the same ciphertext. Same key.

(this is actually a common vulnerability: https://cwe.mitre.org/data/definitions/329.html – we will learn more about this in Lecture 6)

Symmetric Cryptography

In symmetric cryptography, there are two types of ciphers:
stream ciphers and block ciphers. Block ciphers have different modes of operation. Which of the following statements are true?

a) When using a block cipher in ECB mode, the encryption of a block does not include information from any other block.
b) CTR mode is not secure if the nonce is reused under two different keys.
c) When using a stream cipher, both the key and the initialization vector (IV) must be kept secret.
d) Integrity violations can always be detected with stream ciphers.

Answer a.
When using a block cipher in ECB mode, the encryption of a block does not include information from any other block.

Wrong answers:
It is not a problem to reuse the nonce under two keys.
The IV is public.
Stream ciphers are vulnerable to bit-flipping attacks, where an attacker can alter the ciphertext by flipping some bits, and producing a different plaintext.

Lausanne-Bern Direct line

The police forces in Lausanne and Bern want to build a new messaging system that allows them to exchange reports about crimes in real time so that suspects can no longer escape to the other city to avoid law enforcement. To achieve its goal, the system needs to relay messages without long delays. The police thus decides to build their messaging system based on a symmetric stream cipher: Every morning, the main precinct in Lausanne sends a policeman in disguise to Bern with a fresh secret key. This key is used during the whole day for all messages sent between the two cities.
Messages have the following format and headers:

```
Date: <date of crime>
Crime: <type of crime>
Suspect name: <name>
Case description: <free text describing what happened>
```

Théo the Thief, that often operates in Lausanne, reads about the new messaging system in the newspaper Le Temps and thinks "Oh no! I won't be safe in Bern, as the Bern police will also be looking for me!"

Do you agree or disagree with Théo's statement? Justify

1) depending on the communication channel, messages to Bern police can be dropped on the go
2) if they cannot just delete the messages (e.g. ACK system) then tamper with messages since no integrity -> bad
3) key exchange can be tampered with (strong assumption but if justified, ok)

Conclusion: this system is not secure and Theo is safe.