CMPE583 Cybersecurity Homework 1

Yaşar Berkay Taçyıldız

March 2018

1 Solutions

2 Question 2

2.1 ECB (Electronic Codebook Mode)

In ECB plain text is divided into equally sized blocks and each block is encrypted with the same key. Since different parts are encrypted with the same key, plain text can be extracted by frequency analysis. For instance, most frequent letters in English can be identified and matched with most frequent letters in cipher data.

Since, if a block in cipher text is corrupted in ECB, in decryption only modified block will be different than the plaintext.

In case of integrity, when data size increases, it will be difficult to detect if any part of the data is manipulated.

2.2 CFB (Cipher Feedback Mode)

In CFB, firstly IV (initializing vector) is specified and encrypted with the key. Afterwards, output will be XOR'ed with the first plain text block. Cipher text will be used in place of IV for the following blocks.

If any block of cipher text is corrupted in this scheme, following two blocks of plain text will be different, and the rest will remain unchanged.

2.3 OFB (Output Feedback Mode)

In OFB, encryption and decryption operations are identical because the nature of usage location of XOR calculation. In case of encryption, firstly IV and key will be encrypted then the output will be XOR'ed with the plain text block. As the feedback for the following blocks, output of encryption of IV and key is provided. (In decryption, only plain text part can be replaced with cipher text)

Since both plain text and cipher text are not utilized for feedback operation, corruption will only remain same plain text block while decrypting.

2.4 CBC (Cipher Block Chaining Mode)

In CBC encryption, firstly IV is utilized for the encryption of the first block. Then IV and plain text will be XOR'ed, afterwards output will be encrypted with the key. In the case of CBC cipher text will be utilized as IV in the first block.

Corruption of cipher text block, when decrypted, will cause following plain text blocks different than the original plain text.

3 Question 3

3.1 A single character message attack for Apple Devices through WhatsApp

Availability: Since this attack prevents users to access most of the messaging apps due to the submitted special characters to messaging apps, availability is a major issue.

3.2 Nearly Half of the Norway Population Exposed in Health Care Data Breach

Confidentially: Sensitive health-care information should stay confidential.
Integrity: If the attackers can stole health information of the patients, they can also modify them.
Availability: In order to investigate and prevent further data leak, the services of RHF might have been closed temporary. This is an availability issue.
Authentication: Attackers have breached in to Health South-East Regional Health Authority (RHF) in Norway in order to acquire patient information. They have probably bypassed the authentication module of the system.
Privacy: Patients sensitive health information is stolen, which violates privacy.

3.3 Android Trojan Now Targets Non-Banking Apps that Require Card Payments

Confidentially:
Integrity:
Availability:
Authentication:
Access Control:
Non-Repudiation:
Privacy:

3.4 Hard-coded Password Lets Attackers Bypass Lenovo's Fingerprint Scanner

Confidentially:
Integrity:
Availability:
Authentication:
Access Control: Finger print access control mechanism is violated.
Non-Repudiation:
Privacy:

4 Question 4

RC4 algorithm is implemented in NodeJS which is a JavaScript framework. In order to run NIST randomness test condition, a NPM(Node Package Manager) package called nist-randomness-test-suite is utilized.

Result of NIST randomness test is below,

NIST test suite frequencyTest(bits) RC4 should pass frequencyTest (Failed)
perfect generator should pass frequencyTest (224ms) (Passed)
zero biased generator should fail frequencyTest (188ms) (Passed)
faulty generator should fail frequencyTest (177ms) (Passed)
runsTest(bits) RC4 should pass runsTest (Failed)
perfect generator should pass runsTest (192ms) (Passed)
zero biased generator should fail runsTest (123ms) (Passed)
faulty generator should fail runsTest (122ms) (Passed)
nonOverlappingTemplateMatchingTest(bits) RC4 should pass nonOverlappingTemplateMatchingTest (Passed)
perfect generator should pass nonOverlappingTemplateMatchingTest (313ms) (Passed) binaryMatrixRankTest(bits) RC4 should pass binaryMatrixRankTest (Passed)
perfect generator should pass binaryMatrixRankTest (422ms) (Passed)
faulty generator should fail binaryMatrixRankTest (128ms) (Passed)

https://www.npmjs.com/package/nist-randomness-test-suite.