Universität des Saarlandes
Lehrstuhl für Softwaretechnik
Prof. Andreas Zeller, Stephan Neuhaus
Design of Secure Software Systems
Exercise 10

Total number of points obtainable: 21, plus 4 bonus points.

1 Electronic Codebook Mode

(4 points) A database has records encrypted using a block cipher in ECB mode. All records are encrypted with the same key. You are hired to solve the problem of substitutable ciphertext, under the following constraints:

- You must keep the cipher and you must continue to use ECB.
- All records must be encrypted using the same key.
- You may rearrange the records or change their length.
- You need not prevent unauthorized modification of records, but you must be able to detect it. It suffices that you detect the modification of a record; you don't have to detect exactly where the modification occurred.

How would you proceed?

2 Other Modes

2.1 Cipher Block Chaining

Keeping the IV the Same. **(4 points)** We said in the lecture that security was generally unaffected if we chose the same IV for each message, but that there were exceptions. Name one.

Garbling Ciphertext Blocks. **(3 points)** Assume that ciphertext block C_j is garbled due to a transmission error ($0 \leq j \leq n$, where C_0 is the IV). Prove that only plaintext blocks P_j and P_{j+1} are affected by this (if $j = 0$, only P_1 is affected). Assume that the garbled ciphertext block C'_j differs from the original block C_j by δ, i.e., $C'_j = C_j \oplus \delta$. What is the difference in the affected plaintext block P'_{j+1}?

Random Access Decryption with CBC. **(3 points)** Assume you have a random-access file that is encrypted with CBC. Explain how you can decrypt block n without having first to decrypt blocks 1 through $n-1$. Is this also possible for other modes?

Rearranging Ciphertext Blocks **(4 points)** Assume that a message $m_1|m_2|m_3$ is encrypted in CBC and yields the ciphertext $c_0|c_1|c_2|c_3$, where c_0 is the IV. Assume that the ciphertext blocks are rearranged to $c_3|c_2|c_1|c_0$. What will the decrypted plaintext blocks be, in terms of m_i and $D(c_i)$?

2.2 Feedback and Related Modes

Decryption. **(1+1+1 points)** Draw a diagram that depicts the decryption process with CFB, OFB, and CTR modes.

3 Hash Functions and MACs

3.1 Collisions

MACs With Hashes. **(4 bonus points)** We saw that hash$(K_{AB}|m)$ wasn't a good MAC. We also saw that hash$(m|K_{AB})$ would probably work, even though it suffers from a collision problem. Could we send hash$(K_{AB}|m|K_{AB})$ to get the collision resistance of the former plus the tamper resistance of the latter?