Secure and Dependable Systems
Jacobs University Bremen
Dr. Jürgen Schönwälder

Course: CO21-320203
Date: 2018-04-17
Due: 2018-04-24

SADS 2018 Problem Sheet #4

Problem 4.1: *substitution-permutation network* (4+2+3 = 9 points)

Consider a substitution-permutation network implementing an 8-bit block cipher with keys of a length of 32 bits.

The substitution step uses 4-bit S-boxes applied to the lower and upper 4 bits of an 8-bit word. The substitution $S : \{0,1\}^4 \mapsto \{0,1\}^4$ is given by $x \mapsto ((x+1) \cdot 7) \bmod (17-1)$. This is a bijection of $\{0,1\}^4$, where 4-bit chunks are seen as natural numbers via their binary encoding.

The permutation step uses an 8-bit P-box $P : \{0,1\}^8 \mapsto \{0,1\}^8$, which does a cyclic 2-bit left-shift of its argument.

The substitution-permutation network uses the following rounds:

- Round 0: Key step with the first (most significant) 8 bits of the key.
- Round 1: Substitution step followed by a permutation step follows by a key step with the next 8 bits of the key.
- Round 2: Substitution step followed by a permutation step follows by a key step with the next 8 bits of the key.
- Round 3: Substitution step followed by a key step with the last (least significant) 8 bits of the key.

a) Encrypt the cleartext “aba” (0x616261) in electronic codebook mode with the key 0x98267351.

b) Encrypt the cleartext “hello world” (0x68656c6c6f20776f726c64) in cipher block chaining mode with the key 0x98267351 and the initialization vector 0x42.

c) Decrypt the ciphertext 0x3451f6fd3b6126e0ae5815 which has been produced using cipher block chaining mode with the key 0x98267351 and the initialization vector 0x42.

While the calculation can in principle be done on paper, it may be more instructive for computer science students to write a small C program to implement the block cipher and the modes of operation. If you write a C program, please hand it in so we may be able to check where your calculation goes wrong. And recall what we talked about at the beginning of the semester: consider to write test cases to make sure your program is at least handling your test cases correctly.

Problem 4.2: *proof of work* (1 point)

Cryptographic hash functions can be used for a proof of work, also known as a cryptographic puzzle. The challenge is to find a random value that appended to a given message causes the the hash value to have a certain format, e.g., N leading bits of 0.

Your task is to find a random sequence of 64 ASCII letters or digits where the SHA-256 checksum begins with 12 bits (three digits in hexadecimal notation) of 0s. (Since your result is a random solution, we expect it to be different from the results produced by other students.)