Secure and Dependable Systems
Jacobs University Bremen
Dr. Jürgen Schönwälder

Module: CO-566
Date: 2022-03-17
Due: 2022-03-24

SADS 2022 Problem Sheet #6

Problem 6.1: *feistel network* (3+3 = 6 points)

Consider a Feistel Network using 8-bit block and three rounds. The function F adds the round key to a bit block (addition with overflows discarded). Carry out the following calculations on paper.

a) Given the 8-bit cleartext block $m = 01100001$ and the key $k = (k_0, k_1, k_2) = (9, 5, 3)$, calculate the 8-bit ciphertext block.

b) Given the 8-bit ciphertext from a) and the same key k, calculate the 8-bit cleartext.

Problem 6.2: *substitution-permutation network* (3+1 = 4 points)

We define a substitution-permutation network implementing an 8-bit block cipher with keys of a length of 32 bits. We call this cipher *sads crypt*, or short *scrypt*.

- The key step takes 8 bits from the key and performs a bitwise exclusive or with current 8-bit value.
- The substitution step uses 4-bit S-boxes applied to the lower and upper 4 bits of an 8-bit word. The substitution $S : \{0,1\}^4 \to \{0,1\}^4$ 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 $P : \{0,1\}^8 \to \{0,1\}^8$, 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 followed by a key step with the next 8 bits of the key.
- Round 2: Substitution step followed by a permutation step followed 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) Complete the file `scrypt.rs` by implementing the missing functions.

```rust
pub fn enc(m: u8, k: u32) -> u8 {
    todo!();
}

pub fn dec(c: u8, k: u32) -> u8 {
    todo!();
}

pub fn enc_ecb(m: &mut [u8], k: u32) {
    todo!();
}
```

```
pub fn dec_ecb(c: &mut [u8], k: u32) {
    todo!();
}

pub fn enc_cbc(m: &mut [u8], k: u32, iv: u8) {
    todo!();
}

pub fn dec_cbc(c: &mut [u8], k: u32, iv: u8) {
    todo!();
}
```

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