Assignment 4

Exercise 1:

A

A → B: “I’m Alice. Let’s talk”
B → A: N_B (E vangt N_B op)
A → E: K_{AB} {N_B}, N_A
E → B: K_{AB} {N_B}, N_E
B → E: K_{AB} {N_B}

B

A → B: “I’m Alice. Let’s talk”
B → E: N_B (Eve stopt dit bericht)
E → A: N_E
A → E: K_{AB} {N_E}, N_A

C

Als B de encryptie van N_B stuurt, en A dan de encryptie van N_B + 1 terugstuurt is dit protocol veilig(er):

A → B: “I’m Alice. Let’s talk”
B → A: K_{AB}{N_B}
A → B: K_{AB} {N_B+1}, K_{AB}{N_A}
B → A: K_{AB} {N_A+1}

Exercise 2:

A

A → B: hello
B → A: B, K_{AB}{B}
E(B) → A: B, K_{AB}{B}
A → E(B): A, K_{AB}{A}

B

Het is onmogelijk om dit protocol te breken omdat de noncen die er in zitten er voor zorgen dat Eve het protocol niet kan replayen.

C

In dit protocol heeft Eve in het begin de encryptiesleutel al omdat de plain tekst, en de encrypted tekst tegelijk door A verzonden worden.

D

Dit protocol is ook veilig omdat wordt gewerkt met het optellen of aftrekken van 1 bij de encryptie. Hierdoor wordt een hele andere encryptietekst gemaakt dan dat zou ontstaan als alleen de plaintekst wordt geencrypt.

Exercise 3:

A

(a) E(A) → B: A, N_A
(a) B → E(A): N_B, $K_{AB}\{N_A + 3\}$
(b) E(A) → B: B, $N_B + 3$
(b) B → E(A): N_C, $K_{AB}\{N_B + 3 + 3\}$
(a) E(A) → B: $K_{AB}\{N_B + 3\}$

B

A → B: A, N_A
B → A: N_B, $K_{AB}\{N_A + 3\}$
A → B: $K_{BA}\{N_B + 6\}$

C

(a) A → B: A, $K_{AB}\{N_A - 1\}$
(a) B → A: N_A, $K_{AB}\{N_B - 1\}$
(b) E(A) → B: A, $K_{AB}\{N_B - 1\}$
(b) B → E(A): N_B, $K_{AB}\{N_C - 1\}$

Zo kan Eve zich voordoen als Bob.

D

Als B een versleuteling van N_A terug stuurt is het protocol weer veilig.