Cryptography and Network Security Vincent Rijmen 29 August 2018 (14.00 h)

Start every question on a new sheet of paper. Write your name on every page.

1. (6/20 marks) Consider the following mode of operation for the AES. Let K be the 128-bit secret key and let IV denote a 128-bit value that is randomly chosen for each new message and transmitted together with the ciphertext. The plaintext is split in blocks of 128 bit each, denoted by P_1, P_2, ... The ciphertext blocks are computed as follows:

$$C_1 = E_K(P_i) \text{ xor } IV$$
$$C_i = E_K(P_i) \text{ xor } E_K(P_{i-1}),\ i = 2, 3, 4, \ldots$$

   Illustrate this mode of operation with a block diagram and discuss the following properties:

   (a) Hiding of repeated messages (what happens when you encrypt two times the same message using the same key, but a different randomly selected value for IV),

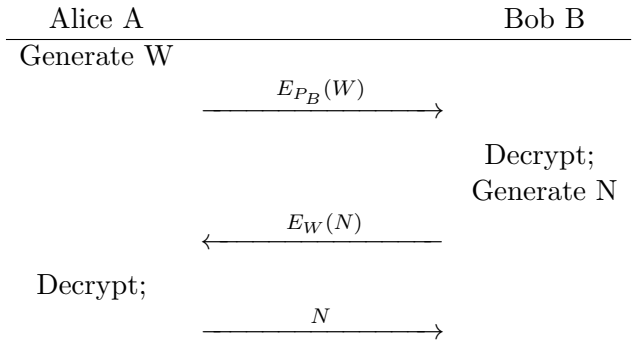
   (b) Hiding of repeated blocks within one plaintext (what happens when you encrypt one message consisting of repetitions of the same block: $P_1 = P_2 = P_3 = \ldots$),

   (c) Error propagation (what happens when a ciphertext bit flips before decryption is started),

   (d) Speed, when compared to CBC mode. Make this comparison both for parallel and for serial computing architectures. Consider both encryption and decryption.

   (e) Is there an upper limit on the number of messages that you can encrypt securely, using the same key but different IV's? Is there an upper limit on the length of a message that you can encrypt securely?

2. (6/20 marks) Consider a protocol where the following messages are exchanged between Alice and Bob.



   Here we used the following notation:

P_B:	the long-term public key of Bob
W:	a random bit string generated freshly by Alice
N:	a random bit string, generated freshly by Bob
$E_x(y)$:	encryption of plaintext y using the key x

   Which goals are achieved by this protocol? Consider implicit key authentication, key confirmation, anonymity to outsiders, key control, forward secrecy and resistance against a known-key attack. Explain. (Where necessary, discuss separately the case for A and for B.)

Please answer also the question on the back of this page.

3. (5/20 marks) Which of the following statements are correct? Point out the errors in the incorrect statements. Explain clearly why the other statements are correct. You get no marks for simply stating "true" or "false"!

   (a) The Dynamic Data Authentication used by some credit cards relies only on public-key cryptography.

   (b) The functions $f3_K$, $f4_K$ used in UMTS can be chosen freely by each UMTS operator.

   (c) When a public-key certificate is revoked, all digital contracts that were signed using the key of this certificate become invalid.

   (d) The salting introduced in the Unix password system was necessary because the original hash function $f()$ used there had an output length of only 64 bits. With a modern hash function, salting is no longer required.

   (e) Messages transmitted over a wire that connects two computers that use both SSL and IPsec, are encrypted twice: once by SSL and once by IPsec. Even if both protocols use AES as encryption algorithm.