Algebra & Security, code 151141, deeltoets Security

Datum : 12-05-2010
Zaal : SP 4
Tijd : 10:45-12:15

1 English

Problem 1.1 (8p):

Demonstrate how Alice and Bob can agree on a shared key using Diffie-Hellman key exchange protocol with system parameters $p = 19$ and $g = 3$ (group generator) if their private keys are $a = 5$ and $b = 7$.

Problem 1.2 (8p):

The parameters of Digital Signature Algorithm (DSA) are given by $p = 47$, $q = 23$ and $g = 4$. Alice's private key is $a = 19$. Prove the correctness of the public parameters of the scheme and compute Alice's public key. Demonstrate the process of signing (by Alice) and verification (by Bob) for a message m with hash value $h(m) = 13$ and ephemeral key $k = 21$.

Problem 2.1 (8p; CBC-4p, CTR-4p):

Consider a block cipher which for a fixed key maps a plaintext to a ciphertext (presented in hexadecimal format) as follows:

Plaintext	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Ciphertext	7	4	A	9	1	F	B	0	C	3	2	6	8	E	D	5

Encrypt the message: $m = (m_1, m_2, m_3, m_4, m_5) = (1, 7, 3, 9, E)$ using CBC mode with $IV = 2$ and using CTR mode with *counter* $= 6$. Work in the binary field, i.e. use the binary presentation of the numbers when xor.

Problem 2.2 (8p):

Consider a block cipher that maps plaintext m_i to ciphertext c_i. Given a message (m_1, m_2, m_3) and his CBC-MAC M, construct another message, which has the same CBC-MAC M. Why this attack is not working for CMAC?

2 Dutch

Problem 1.1 (8p):

Laat zien hoe Alice en Bob een gezamenlijke sleutel kunnen afspreken door gebruik te maken van de Diffie-Hellman key exchange protocol met systeemparameters $p = 19$ en $g = 3$ (groep generator) als hun private keys $a = 5$ en $b = 7$ zijn.

Problem 1.2 (8p):

De parameters van een Digital Signature Algorithm (DSA) zijn gegeven door $p = 47$, $q = 23$ en $g = 4$. Alice's private key is $a = 19$. Bewijs de correctheid van de publieke parameters van het schema en bereken Alice's public key. Demonstreer het process van signeren (door Alice) en verificatie (door Bob) voor een bericht m met hash value $h(m) = 13$ en ephemeral key $k = 21$.

Problem 2.1 (8p; CBC-4p, CTR-4p):

Ga uit van een block cipher met een vaste key die een plaintext naar een ciphertext (gepresenteerd in hexadecimal formaat) als volgt vertaald:

Plaintext	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Ciphertext	7	4	A	9	1	F	B	0	C	3	2	6	8	E	D	5

Encrypt het bericht: $m = (m_1, m_2, m_3, m_4, m_5) = (1, 7, 3, 9, E)$ door gebruik te maken van CBC mode met $IV = 2$ en door gebruik te maken van CTR mode met *counter* $= 6$. Werk in het binaire lichaam, i.e. gebruik de binaire representatie van de getallen tijdens xor.

Problem 2.2 (8p):

Ga uit van een block cipher die plaintext m_i naar ciphertext c_i vertaald. Gegeven een bericht (m_1, m_2, m_3) en bijbehorende CBC-MAC M, construeer een ander bericht die dezelfde CBC-MAC M heeft. Waarom werkt deze aanval niet voor CMAC?