Exercise Sensor Networks

Lecture 10: Security in sensor networks

Exercise 10.1: RSA public key encryption

Prove the multiplicative homomorphic property of RSA

Solution:

Encryption is done by raising the cleartext to the power of the public key and calculating the remainder for the divisor n. n was constructed by multiplying two large primes.

For decryption the ciphertext was again raised to the power of the private key (which is in effect the modulo inverse of the public key) and the remainder modulo n yields the cleartext again.

As we can see, the multiplication of two cleartexts can easily be transformed in the multiplication of thw two corresponding encrypted symbols because either the exponential function as well as the modulo distribute over the multiplication:

$$E(a \times b) = (a \times b)^r \bmod n = (a^r \times b^r) \bmod n = (a^r \bmod n) \times (b^r \bmod n) = E(a) \times E(b)$$

©Thomas Haenselmann – Applied Computer Science IV, University of Mannheim

Exercise Sensor Networks

Lecture 10: Security in sensor networks

Exercise 10.2: Domingo-Ferrer encryption

a) Prove the probabilistic behavior of the Domingo-Ferrer encryption in contrast to the deterministic behavior of RSA using the following values:

d=2, g=28, r=3, and g'=7

Solution:

5 is to be coded. So we decompose 5 into 2+3 or into 1+4 (both is ok).

i) Encrypt (2,3) into ($2x3^1$ mod 28, $3x3^2$ mod 28)=(6, 27)
ii) Encrypt (1,4) into ($1x3^1$ mod 28, $4x3^2$ mod 28)=(3, 8)

Obviously the same cleartext 5 can be encoded into different code words.

(Note that r_{inv}=19)

i) Decode (6,27) into ($6x19^1$ mod 28, $27x19^2$ mod 28)=(2, 3)
ii) Decode (3,8) into ($3x19^1$ mod 28, $8x19^2$ mod 28)=(1, 4)

RSA is deterministic since

(a^p mod n) will always yield the same. There is no random element in the calculation.

b) Prove the additive homomorphic property of the Domingo-Ferrer encryption

©Thomas Haenselmann – Applied Computer Science IV, University of Mannheim

Exercise Sensor Networks

Lecture 10: Security in sensor networks

Exercise 10.2: Domingo-Ferrer encryption

b) Prove the additive homomorphic property of the Domingo-Ferrer encryption

Solution:

Lets encode (a+b):

$E(a+b)=(a+b) \times r \bmod g = (a \times r + b \times r) \bmod g = (a \times r) \bmod g + (b \times r) \bmod g = E(a) + E(b)$

©Thomas Haenselmann – Applied Computer Science IV, University of Mannheim