SECURITY

Assignment 10, Monday, December 11, 2017

S1013793 Carlo Jessurun
S1013792 Tony Lopar
Radboud University

Teaching assistant: Joost Rijneveld

Exercise 1

A. Since the modulo value n of Alice and Bob is the same Alice this means that they also have the same p * q and thus the same φ(n). The value of Bob's private exponent $d_B = e_B^{-1} \bmod (p - 1)(q - 1)$ can be calculated with the public exponent e. Alice may try to find an inverse for all possible e for which holds that $0 < e < \varphi$. If she found a value for d which decrypts in a logical message, she may use this value for all future messages.
B. Usually the value of gcd(p, q) = 1, so since $\gcd(e_A, e_B) = 1$ also holds Eve can use these as values for p and q. Now Eve may use these values to calculate the n for the modulo. Using the extended Euclidean algorithm she may also calculate the inverse of x and y which may be used for decrypting the messages. This method will work since x and y are used to encrypt the message.

Exercise 2

A. We assume here that S does not have to verify the identity of Q, since they already have eachothers keys they (as a group) know who they are.S wants to know sure that he's sending a message to, So, he wants to be sure that the public key is correct. He may use the certificate signed by p $Cert_P(Q)$ to verify the public key of Q since the Pk of P is known by all agents.
B. For the signing of the message S uses his own Sk and anyone knowing the $Pk_{S,}$ can verify this signature. So we need to make sure that W knows the public key of S. We see that the we can verify the signature with $Cert_R(S)$ if we know the Pk_R. We may verify the that we have the right public key of R with $Cert_P(R)$ since we already know the public key of P. This means that we need the following certificates: $Cert_R(S)$ and $Cert_P(R)$.

Exercise 3

We completed the following basic steps to find the plaintext decryption of the 3 blocks:

1. We find the prime factors p and q of n.
2. Then we calculate φ using p−1 and q−1.
3. Using φ and e, we calculate d.
4. Then we now transform the encrypted key to a decimal one to later decrypt it using the above defined d and n.
5. Using this key and the IV, we can decrypt the first block message. I can use the key and the encrypted previous block to decrypt the last 2 blocks
6. Our final step consists of translating this message to plain text.

We wrote down the steps in more detail below:

Action	Result
Already defined data from assignment:	$P_i = D_k(C_i) \oplus C_{i-1}$
	$C_0 = IV$
	n = 9021409837217503169994652443094898049733
	e = 65537
$\varphi = (p-1)\cdot(q-1)$	$\varphi(n) = (81676168843571580071-1)\cdot(110453391300656531123-1)$ $= 9021409837217503169802522882950669938540$
$de = 1 \bmod \varphi(n)$	2511078600645767929925654552860004593113
$M = c^d \bmod n$	897216349798731473416999025202261871445
$c^d \bmod n$ (key!)	76445561849969483702366060490245165073
Hex convert with IV	B4F5556068CE8D5CE1369C6E694F2020 55BB82092A18AAA9EF680A6C2C948F00 **3982E131F0021EFC1BD72FF7AC765011**
$P1 = D_k(C_1) \oplus IV$	01 D3 E7 29 67 79 CD C0 8C 48 5D 03 5E F0 FC 20 **54 68 65 20 4D 61 67 69 63 20 57 6F 72 64 73 20**
$P1 = D_k(C_2) \oplus C_2$	D5 87 30 40 3B BF F8 39 80 5B F5 1D 01 6F 6F 53 **61 72 65 20 53 71 75 65 61 6D 69 73 68 20 4F 73**
$P1 = D_k(C_3) \oplus C_2$	9E F7 A4 6A C6 AB 61 97 CA 29 A4 AD A7 AD BF 02 **73 69 66 72 61 67 65 58 58 58 58 58 58 58 58 58**
Translated to ASCII	**The Magic Words are Squeamish Ossifrage**