How is the message digest related to Signatures and Encryption?

Asked 3 years, 9 months ago Active 11 months ago Viewed 4k times

7

I was studying about 'Data Security' and I found out this one thing confusing.

What is a message digest? I got it is the hash of the message.

Is the message here referring to the plaintext or cipher text? I believe when using Digital Signatures, the message itself is also encrypted with a public key.

5

encryption hash public-key signature

edited Jan 26 at 19:41
Ella Rose ♦
18.1k 5 46 87

asked Mar 21 '16 at 9:01
Hassan Althaf
181 1 5

1 Answer

17

First of all, yes, the message digest is the hash of the message.

Secondly, do not mix things up. You are talking about public key encryption and signature. Let's redefine them to make sure we have everything right.

Alice and Bob got pairs of key (A_{pub}, A_{priv}), (B_{pub}, B_{priv}). Alice knows B_{pub} and Bob knows A_{pub}.

- Alice wants to send a message m to Bob $\implies$ She encrypts it with B_{pub}.
- Alice wants to prove to Bob that it was she who sent the message $\implies$ She signs it with her private key A_{priv}.

How does the message digest appear in all that ? Continue reading.

Problem: signing and encryption using RSA (*standard procedure*) is slow. How to speed up the process ?

1. Alice encrypts the message with a symmetric cipher (*AES*) using a random generated key K_{sym}. Then, encrypt K_{sym} with the B_{pub}.
2. Alice does not sign the message, she signs the message digest. Smaller therefore faster.

All this together ? Here are the steps :

1. Alice hashes the message $m \implies$ she gets the message digest.
   $H(m) \rightarrow MD.$
2. Alice signs MD with her private key.
   $E_{A_{priv}}(MD) \rightarrow Sig.$
3. Alice generates a random key for the symmetric encryption.
   $rdm() \rightarrow K_{sym}$
4. Alice encrypts the message and the signature with a symmetric cypher.
   $E_{K_{sym}}(m||Sig) \rightarrow c$
5. Alice encrypts the symmetric key with Bob's public key.
   $E_{B_{pub}}(K_{Sym}) \rightarrow K_{cipher}$
6. Alice sends (c, K_{cipher}) to Bob.

Remark: It is a good practice to have 2 pairs of keys : one for encryption, one for signatures.

edited Mar 21 '16 at 13:22
Community ♦
1

answered Mar 21 '16 at 9:52
Biv
9,190 2 31 61

Great! It was very useful! I was wondering if it was right to say if symmetric algorithms use the same algorithm and key for both encryption and decryption? – Hassan Althaf Mar 21 '16 at 14:08

symmetric encryption algorithm means that the key is the same for the encryption and the decryption : caesar, AES, DES ... public key encryption (or asymmetric encryption) means that the key to encrypt is different to the key to decrypt. The source code for encryption and decryption is unrelated to the kind (symmetric / asymmetric) : RSA is asymmetric but the same code is used to encrypt and decrypt. DES, AES are symmetric, but you need to specify the mode you want to use. – Biv Mar 21 '16 at 14:39

What is the purpose of also encrypting the signature? – Cocowalla Apr 20 '18 at 9:32