

IT2760/CS3760: Coursework 2

Solutions

1. Explain how, if a CBC-MAC is computed without the Optional process, two one-block messages and MACs can be combined to give a 'bogus' two-block message with a valid MAC. Describe how this approach can be extended to combine two messages of arbitrary length. How does the optional process protect against this attack?

[8 marks]

If the single-block messages m_1 and m_2 have MACs: MAC_1 and MAC_2 respectively, then the correct MAC for the two-block message $(m_1, m_2 \oplus MAC_1)$ is MAC_2 .

Suppose an attacker intercepts two multi-block messages:

(m_1, m_2, \dots, m_q) and $(m'_1, m'_2, \dots, m'_r)$

with MACs MAC_1 and MAC_2 , respectively.

Then the following message containing $q+r$ blocks:

$(m_1, m_2, \dots, m_q, m'_1 \oplus MAC_1, m'_2, \dots, m'_r)$

will have MAC MAC_2 .

The optional process offers protection by 'encrypting' O_q , the final output block in the CBC-MAC construction; as a result, the MAC of one message cannot be combined with the first block of another message in the way described above.

2. State, with an explanation, whether or not the following active attacks can be detected by the use of a MAC:
- Alteration or replacement of a message;
 - Deletion of a message;
 - Insertion of a false message;
 - Replay of an old message;
 - Changing the order of two or more messages;
 - Falsifying the origin of a message.

[12 marks]

Alteration or replacement of a message – *Alteration of a message will alter at least one block of that message. Since all message blocks affect the calculation of the MAC, the original MAC will no longer be valid. A new MAC cannot be computed without knowledge of the key. So the answer is Yes.*

Deletion of a message – Message deletion cannot be detected by an integrity mechanism or any other cryptographic mechanism on its own. Other mechanisms, such as message sequence numbers can be used for protection. No.

Insertion of a false message – A valid MAC cannot be calculated without knowledge of the key, so protection is provided and the attack can be detected. Yes.

Replay of an old message – This attack will not be detected. Non-cryptographic mechanisms are required to prevent replay attacks; freshness mechanisms are used. No.

Changing the order of a message – This attack will be detected since the order in which blocks are ‘chained’ will change the final output. Yes.

Falsifying the origin of a message – It is only possible to claim that a message originates from an entity (X say) if an attacker can generate a MAC for the message using the key shared by X with the recipient. Yes.

N.B. All the above analysis is based on the assumption that the key has not been compromised, in which case all security is lost.

3. **Encryption does not provide message integrity protection.** Describe, with the aid of simple examples, why this is true when a stream cipher is used for encryption. That is, show how an interceptor of a ciphertext message can manipulate the contents of a message without detection and with known effects on the message. Describe, again using a simple example, how much more serious such an attack can be if the attacker knows part of the plaintext for the intercepted ciphertext.

[6 marks]

Suppose an attacker intercepts a 100-bit message encrypted using a stream cipher. Suppose also that the attacker knows that bits 93-100 (i.e. the final eight bits of the message) are used to transmit an 8-bit number (most significant bit first). Then the attacker can flip bit 93 of the ciphertext message, and will know that the recipient will, after decryption, receive the message correctly except that bit 93 will have been flipped. If the number encoded in bits 93-100 was less than 128 (i.e. it had leading bit zero), then the effect will be to add 128 to the number. Contrariwise, if the leading bit of the original number is 1, then the modified message will contain the number reduced by 128.

If the attacker knows some of the original plaintext, then the attacker can recover the keystream corresponding to these known plaintext bits, and can now modify the ciphertext so that the modified plaintext will contain whatever the attacker chooses.

4. What is the main difference between a conventional encryption system and a public key encryption scheme?

[3 marks]

In a conventional scheme the sender and receiver must share a secret key, which must be distributed in a way that preserves its secrecy and integrity. In a public key scheme, the sender must know (in a reliable way) the public key of the receiver, and only the receiver must know his or her private key. Public keys can be distributed through public channels, although their authenticity must be guaranteed.

5. Suppose that RSA is used to encrypt a 2-bit message without any randomisation of the plaintext, and suppose also that an interceptor of the ciphertext knows the plaintext message only contains two bits of data (i.e. it is one of '00' '01', '10' and '11'). Can the cryptanalyst discover the plaintext (suppose that the cryptanalyst knows the public encryption key used to encipher the message), and, if so, how?

[4 marks]

The cryptanalyst can discover the plaintext by simply going through all possible plaintext messages, i.e. 00, 01, 10 and 11, and enciphering each of them using the public encryption key. The cryptanalyst then compares the resulting ciphertext in each case with the intercepted ciphertext. One will match, and this will immediately reveal the plaintext.

[This helps to explain why RSA should not be used to encrypt data without applying a 'randomising' process to the data prior to performing the RSA exponentiation operation.]

6. Distinguish between digital signatures giving message recovery and digital signatures without message recovery.

[4 marks]

In a digital signature giving message recovery, the input to the verification process is simply the signature s (and the public verification key), and the output is a copy of the original message m and an indication (a Boolean) as to whether or not the signature is valid. That is the message can be recovered from the signature.

In a scheme without message recovery, the input to the verification function is the public key, the message m and the signature s , and the output is a boolean indicating whether or not the signature is a valid signature on the message. That is, the message cannot be recovered from the signature.

7. How can RSA be used as the basis of a signature scheme without message recovery? What extra cryptographic functions do you need, and what properties should they have?

[6 marks]

The extra function required is a collision-resistant one-way hash-function. A hash-function $h : M \rightarrow C$ is one-way if, given an arbitrary $c \in C$, it is computationally infeasible to find any $m \in M$ such that $h(m) = c$. A hash-function $h : M \rightarrow C$ is collision-resistant if it is computationally infeasible to find any pair $m, m' \in M$ ($m \neq m'$) such that $h(m) = h(m')$.

Signing using a hash-function involves first applying h to m to get the hash-code $H = h(m)$, and then applying the RSA signature process:

$$s = H^d \bmod n.$$

Verifying a pair $(m; s)$, involves recovering H from s by:

$$H = s^e \bmod n$$

and then verifying that $H = h(m)$.