

2006 Paper 4 Question 10

Introduction to Security

- (a) Alice and Bob participate in a public-key infrastructure that enables them to exchange legally binding digital signatures.
- (i) Name *two* reasons why, for some purposes, Alice might prefer to use a message authentication code, instead of a digital signature, to protect the integrity and authenticity of her messages to Bob. [4 marks]
- (ii) Outline a protocol for protecting the integrity and authenticity of Alice's messages to Bob that combines the benefits of a public-key infrastructure with those of using a message authentication code. [4 marks]
- (b) Your colleague proposes a new way for constructing a message authentication code using a block cipher $E : \{0, 1\}^{64} \times \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$. He takes the n -bit input message M , appends $p = 64 \cdot \lceil n/64 \rceil - n$ zero-bits, and splits the result into $k = (n + p)/64$ 64-bit blocks $M_1 || M_2 || \dots || M_k = M || 0^p$. He then calculates the message authentication code as

$$C_K(M) = E_{M_1}(E_{M_2}(E_{M_3}(\dots E_{M_k}(K) \dots)))$$

where K is the 128-bit secret key shared between sender and recipient. Show *two* different ways in which an attacker who observes a pair $(M, C_K(M))$ can, without knowing K , create a new pair $(M', C_K(M'))$ with $M' \neq M$.

[6 marks]

- (c) Show how a 128-bit message authentication code $C_K(M)$ with 64-bit key K can be constructed for an n -bit long message M using
- (i) a secure hash function $H : \{0, 1\}^* \rightarrow \{0, 1\}^{256}$, such as SHA-256; [2 marks]
- (ii) a block cipher $E : \{0, 1\}^{128} \times \{0, 1\}^{256} \rightarrow \{0, 1\}^{256}$. [4 marks]