Tecnologia Criptográfica

MIEI

1º Teste – 6 de Novembro de 2017

Questão 1

1. Qual o significado da afirmação: *a cifra* one-time-pad *exibe segurança absoluta*.
2. As cifras sequenciais, e em particular as cifras síncronas, acabam por aproximar a cifra *one-time-pad*. É então legítimo afirmar-se que essas cifras exibem o mesmo nível de segurança? Justifique.
3. O modo de operação *Cipher Feedback (CFB)* é caracterizado por:

$$C_0 = IV$$
$$C_i = E_k(C_{i-1}) \oplus P_i$$
$$P'_i = E_k(C_{i-1}) \oplus C_i$$

para um vector de inicialização IV; texto limpo $P = P_1 \cdots P_n$; criptograma $C = C_0 \cdots C_n$; texto recuperado $P' = P'_1 \cdots P'_n$; e onde $E_k(-)$ é a operação da cifra de blocos (com chave k).

   (a) Este modo de operação permite emular uma cifra sequencial a partir de uma cifra por blocos. Explique porquê e quais as características da cifra resultante.

   (b) Parece-lhe que neste modo de operação, basta que o vector de inicialização não se repita (e.g. utilizando um contador)? Justifique.

Questão 2

1. Uma primitiva basilar em criptografia são as *funções de hash* criptográficas. Quais as características que se espera dessa primitiva?
2. Uma aplicação das funções de hash é na construção de *códigos de autenticação* (MAC). A partir de uma função de hash `h`, define-se:

$$\text{HMac}(k, M) = \texttt{h}(k \oplus \text{opad} || \texttt{h}(k \oplus \text{ipad} || M))$$

.

   (a) Que propriedades se espera de um MAC?

   (b) Como é que no HMAC essas propriedades decorrem das atrás enunciadas para as funções de hash?

   (c) Como deve ser usado?

Questão 3 Das formas genéricas de se combinar uma cifra simétrica com um MAC, a que exibe maiores problemas é a `encrypt-and-mac`. Explique no que consiste e que problemas lhe são apontados.

Questão 4 Considere a seguinte variante do protocolo *Diffie-Hellman* onde a operação de exponenciação modular é substituída pela multiplicação modular: (fixando um primo p e um gerador g):

A→B: $+x;\ (g \times x)[p]$

B→A: $+y;\ (g \times y)[p]$

A: $K = (((g \times y)[p]) \times x)[p] = (g \times x \times y)[p]$

B: $K = (((g \times x)[p]) \times y)[p] = (g \times x \times y)[p]$

Podemos esperar que esta variante satisfaça as mesmas garantias de segurança que o protocolo original? Justifique.