Exercises on hash functions and MACs

Exercise 6.5: Give an example of a hash function that is presumably preimage resistant, but not second preimage resistant.

Exercise 6.6: Define a hash function h to hash n-bit strings to m-bit strings (it is then a compression function). Assume h is constructed as $h : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ through

$$h(x) = ((\sum_{i=0}^{d} a_i x^i) \bmod 2^n) \bmod 2^m,$$

for some fixed d and coefficients $a_i, i = 0..d$. Show how you solve the second preimage problem without solving some polynomial equation.

Exercise 6.7: Assume we have a hash function h_1 (compression function) mapping $\{0,1\}^{2m}$ to $\{0,1\}^m$, i.e., compressing $2m$ bits to m bits. Assume furthermore that h_1 is collision resistant. Now construct a new hash function h_2 mapping $\{0,1\}^{4m}$ to $\{0,1\}^m$, i.e., compressing $4m$ bits to m bits, by

$$h_2(x) = h_2(x_1||x_2) = h_1(h_1(x_1)||h_1(x_2)),$$

where $x \in \{0,1\}^{4m}$ is written as $x = x_1||x_2$, $x_1, x_2 \in \{0,1\}^{2m}$ and $||$ means bitstring concatenation.

Prove that h_2 is collision resistant.

Exercise 6.8: [difficult] Consider the generation of b-bit MACs through CBC-MAC (slide 5, lec15). The MAC is denoted as $MAC(x,k)$, where $x = x_1 x_2 \ldots x_n$, and k is the secret key, and generated by computing $y_i = E_k(y_{i-1} \oplus x_i)$ and finally setting $MAC(x,k) = y_n$. The block size is b bits.

Assume that Eve can get Alice to generate the MACs for about $q = 2 \cdot 2^{b/2}$ different messages of her choice. Show how she can then find a correct MAC (that is correctly verified by Bob) for a new message for which Alice never generated a MAC.

Hint: For the q messages, let x_1 run through q different values, let x_2 be randomly chosen and let $x_3, \ldots$ be the same for all messages. Then use birthday paradox arguments.