Security

Assignment 3, Wednesday 24 September 2008

Goals: After successfully completing this exercise you should be familiar with Vigenere Chipers and be able to identify properties of cryptographic hashes and one-time pads.

Deadline: Friday October 3rd, during the lecture or earlier in Flavio's or Olha's post box (in the white cabinet near the printer at the station-side-end of the corridor on the second floor of the Huygens building).

A cryptographic hash is a function h that assigns to a bit string another bit string (usually of fixed length, but this is not a formal requirement here), and has the following three properties:

(E) h can be computed efficiently,

(O) given a bit string y it is infeasible to determine a bit string x such that $h(x) = y$ (onewayness),

(C) it is infeasible to determine two bit strings x, x' such that $h(x) = h(x')$ (collision resistance).

A (4 points) Given a function H that meets (E), (O) and (C), determine for the following functions h which of the demands apply

- The function $h(x) = 1$. (The function h returns constant output.)
- The function $h(x) = x$. (The function h always returns its input unchanged.)
- The function $h(x_1 \cdots x_{2n}) = (x_1 \text{ XOR } x_{n+1}) \cdot (x_2 \text{ XOR } x_{n+2}) \cdots (x_n \text{ XOR } x_{2n})$, where x_i are the individual bits of the input. (The function h computes the bitwise exclusive or of the first and the second half of its input.)
- The function $h(x_1 \cdots x_n) = H(x_1 \cdots x_{48}) \cdot x_{49} \cdots x_n$, where x_i are the individual bits of the input bit string. (The function h hashes the first 48 bits of its input using H, and appends the rest of its input unchanged to the end of the result of H)
- The function $h(x_1 \cdots x_{2n}) = H(x_1 \cdots x_n) \cdot x_{n+1} \cdots x_{2n}$, where x_i are the individual bits of the input bit string. (The function h hashes the first half of its input using H, and appends the rest of its input unchanged to the end of the result of H)

B (4 points) One way to construct a one-time pad uses a hash function h and starts with an initial key K and appends iterated applications of h:

$$K \cdot h(K) \cdot h(h(K)) \cdot h(h(h(K))) \cdots$$

- Which of the three properties (E), (O), (C) of h is used? Motivate your answer.
- Is this way to construct a one-time pad secure? Motivate your answer.
- (Optional) Can you think of a better construction using only hash functions?

C (2 points) Find out how Vigenere Chipers work. Encrypt the following plaintext (corresponding to declarations of George Bush in an interview at the 2008 Olympics, Beijing, Aug. 10, 2008):

```
I DONT SEE AMERICA HAVING PROBLEMS
```

using the key `BUSH`.