Security

Assignment 2, Wednesday 17 September 2008

Goals: After successfully completing this exercise you should be able to break simple substitution and transposition ciphers; you know how to use one-time pads. The first task is to repeat what we have learned and done earlier.

Deadline: Friday September 26, 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 (2 points) Albert Heijn has recently started an experiment where customers can pay with fingerprints, see e.g.:
http : *//www.nu.nl/news/*1616308/37/*V ingerbetaling_bij_supermarkt.html*

(a) Explain why non-repudiation is a relevant security property in this situation

(b) Do fingerprints guarantee non-repudiation?

(c) Which privacy guarantees do you think that Albert Heijn should give to its customers in this experiment?

(d) Optionally: what do you think of this experiment?

B (3 points) [Similarly to Tanenbaum, 8.1, but the key and the plain text are changed!] Break the following mono-alphabetic cipher. The plain text, consisting of letters only, is an English text.

kqe w ygn bi hqek sq myiir
rcgn sti yqch bn mqay sq uiir
wj w hwi xijqci w egui
rcgn sti yqch bn mqay sq sgui

tamt ywssyi xgxn, hq kqs mgn g eqch
gkh kidic bwkh stgs kqwmi nqa tigch
wsm zams sti xigms akhic nqac xih,
wk nqac pyqmis, wk nqac tigh

Explain how you did it.

C (3 points) [Tanenbaum, 8.2.] Break the following columnar transposition cipher (see Tanenbaum 8.1.3).

aauan cvlre rurnn dltme aeepb ytust iceat npmey iicgo gorch srsoc nntii imiha oofpa gsivt tpsit lbolr otoex

Explain how you did it. The plain text consists of letters only (no spaces), but is displayed here in groups of five for readability. Hint: the plain text comes from a Computer Science text book, so computer is a word that is likely to occur often.

D (2 points) Translate the plain text "Alice+Bob" to binary values via 7-bits ASCII. Find a 63-bits one-time pad which yields the cipher text below:

ASCII	A	l	i	c	e	+	B	o	b
binary	1000001	1101100	1101001	1100011	1100101	?	?	?	?
pad	?	?	?	?	?	?	?	?	?
ciphered	1011001	1101111	0000101	0110000	0110010	0010000	0001110	1001111	1100101