

M360 Mathematics of Information Security

exercise sheet # 7

Exercise # 1

(1 points)

Naive Nelson uses RSA to receive a single ciphertext c , corresponding to the message m . His public modulus is n and his public exponent is e . Since he feels guilty that his system was used only once, he agrees to decrypt any ciphertext that someone sends him, as long as it is not c , and return the answer to that person. Evil Eve sends him the ciphertext $2^e c \bmod n$. Show that this allows Eve to find m .

Exercise # 2

(1 points)

Consider the groups (U_n, \cdot) . Is U_8 cyclic? What about U_{10} ?

Exercise # 3

(1 points)

Prove by setting up truth tables: $A \iff B \equiv \neg A \iff \neg B$

Exercise # 4

(7 = (1 + 1 + 1) + (1 + 1 + 1 + 1) points)

Check whether the following arguments are logical or not. Explain!

- a)
- i) If Alice is wrong, then Bill is wrong. If Bill is wrong, then Connie is wrong. Connie is wrong. Therefore, Alice is wrong.
 - ii) If turtles can sing, then artichokes can fly. If artichokes can fly, then turtles can sing and dogs can't play chess. Dogs can play chess if and only if turtles can sing. Therefore, turtles can't sing.
 - iii) If I oversleep, I will miss the bus. If I miss the bus, I'll be late for work unless Sue gives me a ride. If Sue's car is not working, she won't give me a ride. If I am late for work, I'll lose my job unless the boss is away. Sue's car is not working. The boss is not away. Therefore, if I oversleep, I'll lose my job.
- b) And a selection from Lewis Carroll:
- i) No ducks waltz. No officers ever decline to waltz. All my poultry are ducks. Therefore, my poultry are not officers.
 - ii) Everyone who is sane can do Logic. No lunatics are fit to serve on a jury. None of your sons can do Logic. Therefore, none of your sons are fit to serve on a jury.
 - iii) The only articles of food, that my doctor allows me, are such as are not very rich. Nothing that agrees with me is unsuitable for supper. Wedding-cake is always very rich. My doctor allows me all articles of food that are suitable for supper. Therefore, wedding-cake always disagrees with me.
 - iv) Animals, that do not kick, are always unexcitable. Donkeys have no horns. A buffalo can always toss one over a gate. No animals that kick are easy to swallow. No hornless animal can toss one over a gate. All animals are excitable, except buffaloes. Therefore, donkeys are not easy to swallow.

due Friday, 10/28/05.