

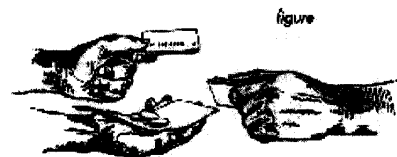
Toegepaste Wiskunde 314

Taak 1: Kriptologie (2004)

Figuur 1 toon 'n bladsy van die gebruikershandleiding van 'n *Taurus STS* muureenheid wat in huise gebruik word om die aankoop van elektrisiteit te administreer. Die gebruiker ontvang saam met die muureenheid 'n unieke kaart (baie soos 'n bankkaart) waarop die reeksnommer van die muureenheid (op die kaart se magneetstrook) gestoor is. Om krag te koop, neem die gebruiker die magneetkaart na die munisipale kantoor en betaal daar per eenheid vir die elektrisiteit wat hy in sy huis beskikbaar wil hê. Ná betaling ontvang die gebruiker 'n 20-syfer getal wat hy dan tuis op die muureenheid moet intik om die krag beskikbaar te stel. Hierdie 20-syfer getal is gebaseer op die reeksnommer van die muureenheid (afkomstig van die magneetkaart), sodat die kode ongeldig is vir gebruik in enige ander huis as die gebruiker s'n. Verder bevat die 20-syfer kode ook inligting aangaande die hoeveelheid krag wat by die munisipale kantoor gekoop is, en is die kode net geldig vir eenmalige gebruik. Daar is ook 'n vervaldatum by die 20-syfer kode ingesluit wat eerste gebruik van die kode beperk tot 3 maande ná die betaaldatum. Figuur 2 toon die

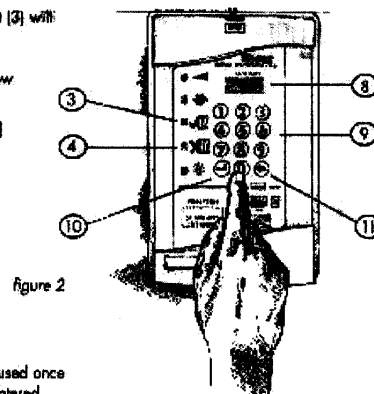
How to use your Energy Dispenser

Your User I.D. Card (12) must be given to the vendor with your money (figure 1). He will return your I.D. Card with your credit token.



Key in your credit token using the keypad (9) (figure 2). Check the display window (8). If incorrect, press "Backspace/Delete" key (11) to remove number and re-key correct code.

2. Push "Enter" key (10).
3. The "Code Accepted" light (3) will flash and total available credit (8) is displayed. The energy dispenser is now ready for use.
4. If "Code Rejected" light (4) flashes, re-enter the code.



N.B. Each code can only be used once and will display "Used" if re-entered.

Figuur 1

moontlike boodskappe wat op die vertoonvenster van die eenheid kan verskyn.

Gebruik u kennis van publieke sleutel stelsels om te toon hoe die bogenoemde sisteem met behulp van die RSA-kriptosisteem kan werk.










Ontwerp u eie weergawe van so 'n betaalstelsel en illustreer dit aan die hand van 'n voorbeeld (u kode hoef nie 20 syfers lank te wees nie!). Maak seker dat u ontwerp voorsiening maak vir:

- 'n beperking op die gebruik van 'n kode tot die regmatige muureenheid.
- 'n eenmalige gebruik van elke kode.
- 'n vervaldatum van elke kode.
- 'n boekhouding van die hoeveelheid kragenhede wat gekoop is en dus op die vertoonvenster moet verskyn.

Hoe maklik sal dit vir 'n gebruiker van u sisteem wees om 'n geldige kode onregmatig uit te dink, en dus elektrisiteit te ontvang sonder om daarvoor te betaal?

Problem Solving

1. If your token has not been accepted by the meter, report to vendor.
2. If the display shows:

	(blank) - call your supplier
	no credit - you will not be able to use electricity until extra credit is loaded
	the token has been accepted
	the token has been rejected - try again
	the token is old and is no longer valid
	the token has already been used and is no longer valid
	power overload - switch off some circuits and wait for the electricity to be reconnected (± 30 seconds)
	power overload - call your supplier
	call your supplier

Every effort has been made to ensure that the information in this document is complete, accurate and up to date. Schlumberger assumes no responsibility for the results of errors beyond its control. Schlumberger also cannot guarantee the successful operation of any products used with this product other than those manufactured by Schlumberger.

Figuur 2