p896
RJA

2004

Model answer - security II - second question

(a) $N_C = 40$ bits and $N_R = 24$ bits

Reason: if $N_C = N_R = 32$ bits and the valet builds a table of 36,000 (N_C, N_R) pairs - an hour's work - then the number of trials needed at the car is $2^{32}/36{,}000 = 119{,}304$ which at 3,600 per hour is ~33 hours. The protection is marginal.

However if $N_C = 40$ bits then one hour of collection leads to 8483 hours of trials. A weekend of trials - 60 hours, say - would ~~to~~ need 141 hours of data collection at the hotel. Not perfect but much better.

(Best is maybe 21 bits but depends on balance between valet attack and exhaustive attack - should on principle make the latter harder so 24 a good choice)

(c) Generate the N_C by encrypting a counter
$N_C = \{count\}_{K'}$ where k' is another key

(d) All that a password generator does in this context is to force the phisher to do his middleperson attack in real time. This is not all that serious a constraint. So I would not be enthusiastic.

(b) No; keysearch isn't The easiest attack