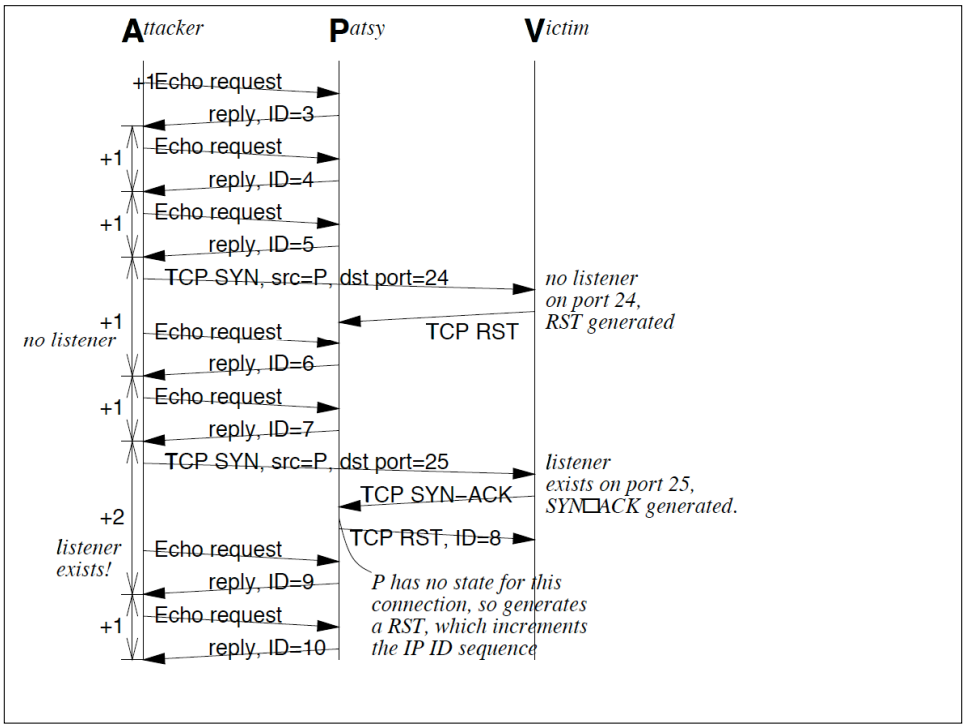
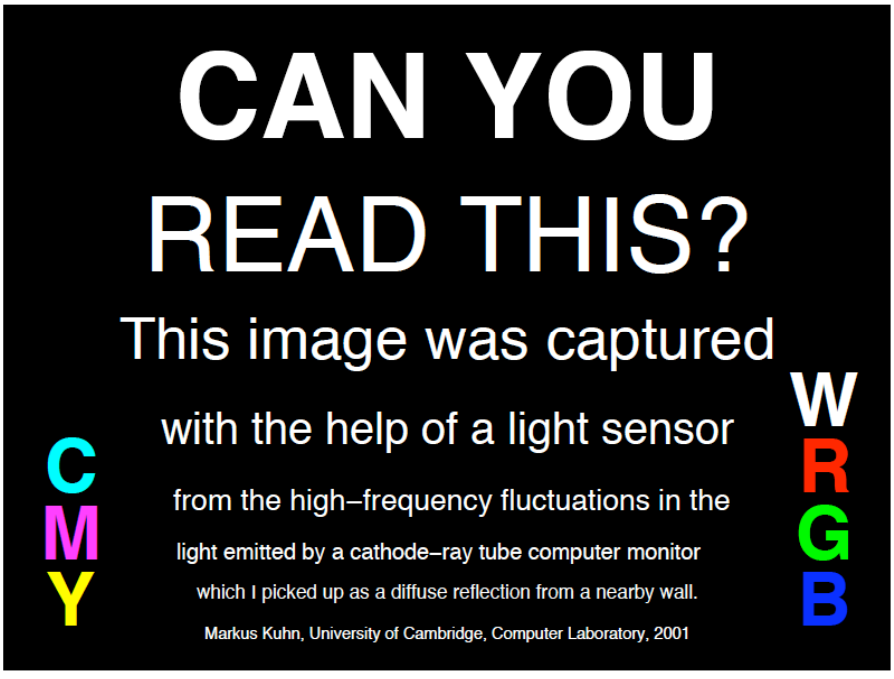

Attacker
Patsy
Victim
+1
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener on port 24, RST generated
TCP RST
+1
no listener
Echo request
reply, ID=6
+1
Echo request
reply, ID=7
TCP SYN, src=P, dst port=25
listener exists on port 25, SYN□ACK generated.
TCP SYN–ACK
+2
TCP RST, ID=8
listener exists!
Echo request
reply, ID=9
P has no state for this connection, so generates a RST, which increments the IP ID sequence
+1
Echo request
reply, ID=10


CAN YOU
READ THIS?
This image was captured
with the help of a light sensor
from the high–frequency fluctuations in the
light emitted by a cathode–ray tube computer monitor
which I picked up as a diffuse reflection from a nearby wall.
Markus Kuhn, University of Cambridge, Computer Laboratory, 2001
C
M
Y
W
R
G
B

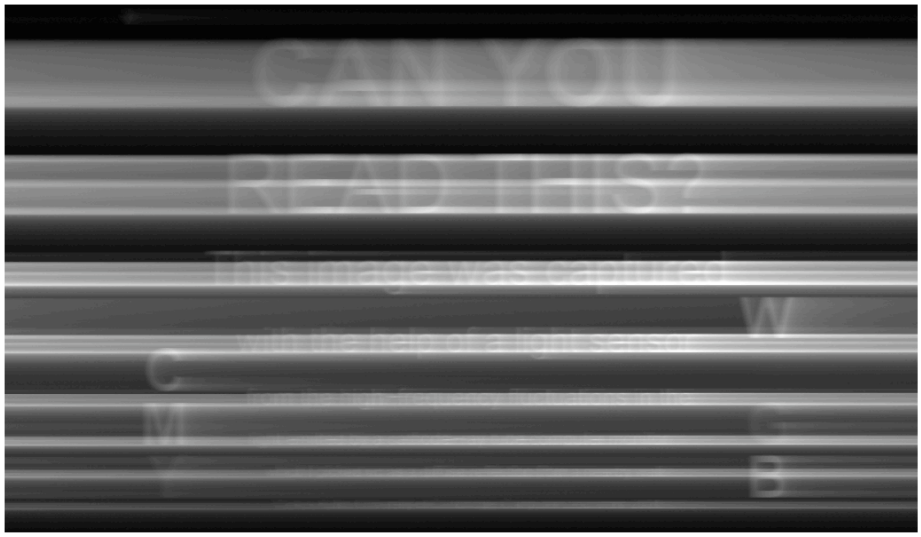


Figure 6.9: Unprocessed photomultiplier output after diffuse reflection from a wall

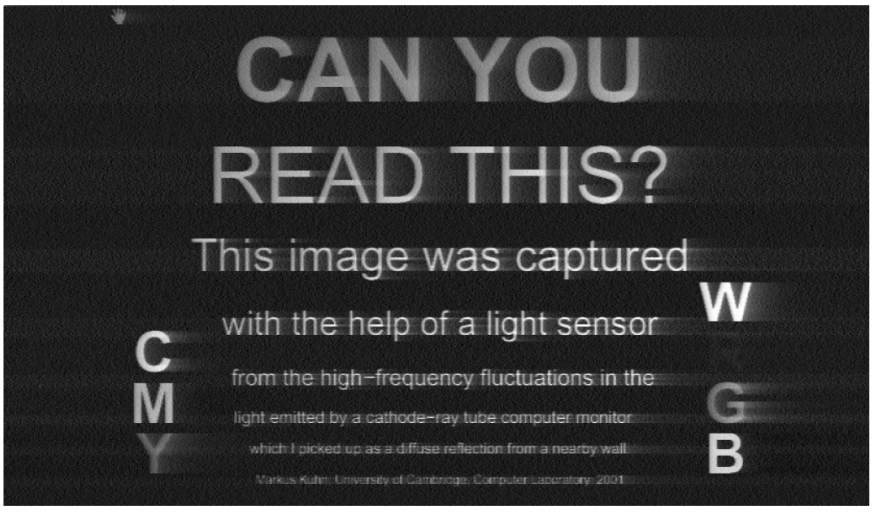


Figure 6.11: A much better image quality can be achieved by applying a matched filter with a frequency characteristic that is inverse to that of white shown in Fig. 6.7.

Figure 6. Reflections in two other tea pots, taken from a distance of 5m. The 18pt font is readable from the reflection in the left picture, and almost readable in the right picture.

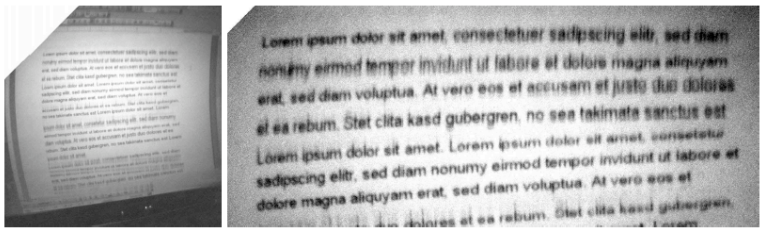


Figure 7. Reflection of a Word document with small 12pt font size in a tea pot, taken from a distance of 5m. The 12pt font is readable from the reflection.

Figure 9. Image taken with a macro lens from very short distance, with realistic distance between the monitor and the eye. Readability is limited by the resolution of the camera.

Figure 10. Reflections in two different pairs of glasses, taken from a distance of 5m. Both the inner side and the outer side of glasses produce reflections. The 18pt font is readable from the reflection.

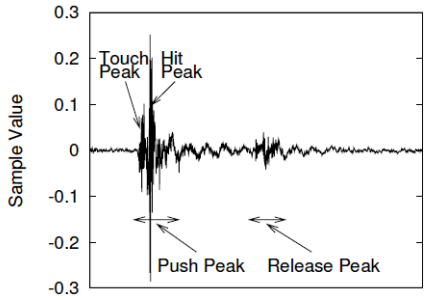


Figure 3: The audio signal of a keystroke.

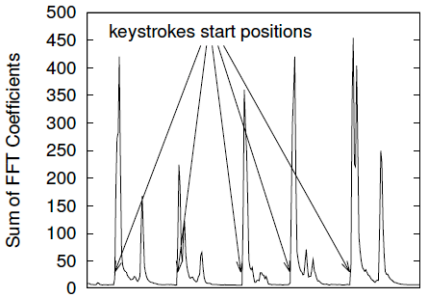


Figure 4: Energy levels over the duration of 5 keystrokes.

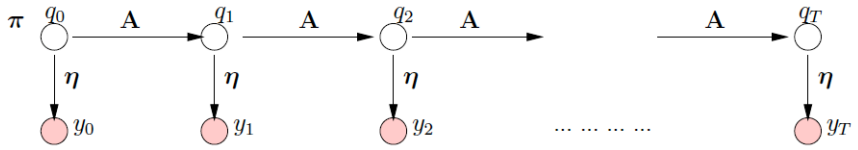
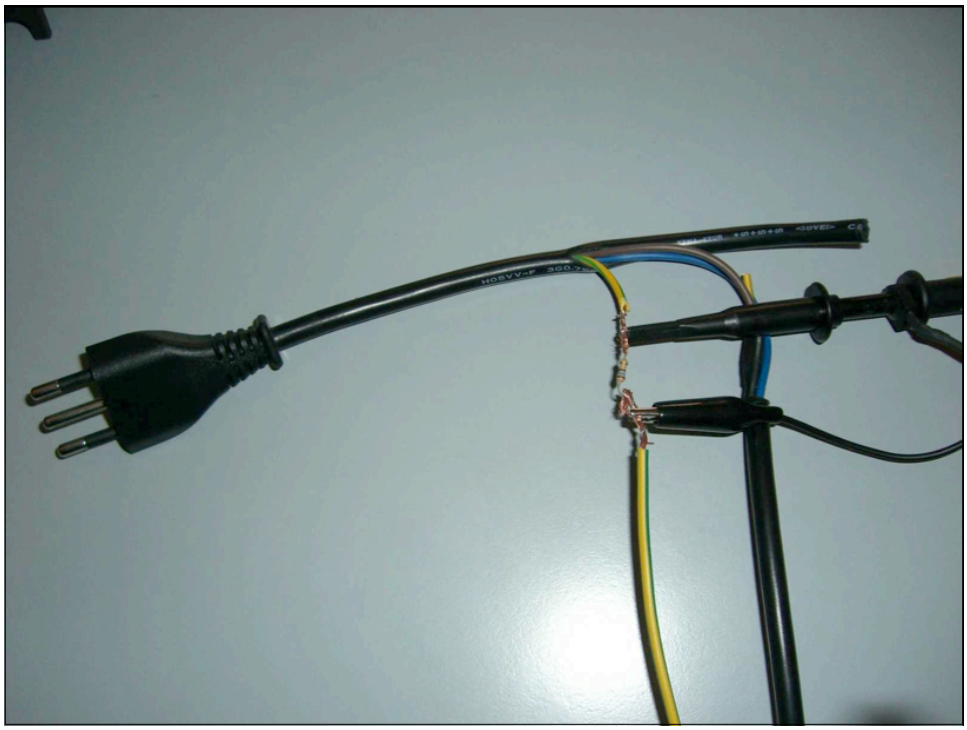


Figure 5: The Hidden Markov Model for unsupervised key recognition.



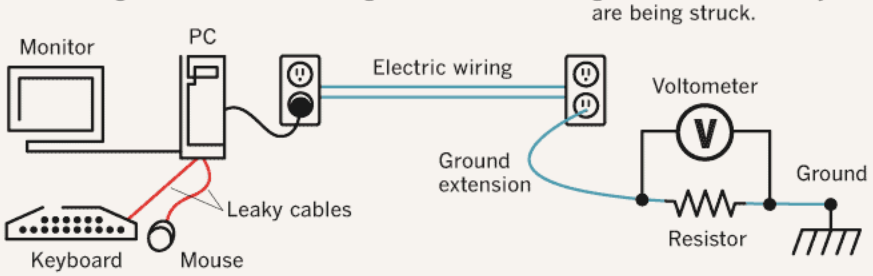
Stealing keystrokes through electric lines

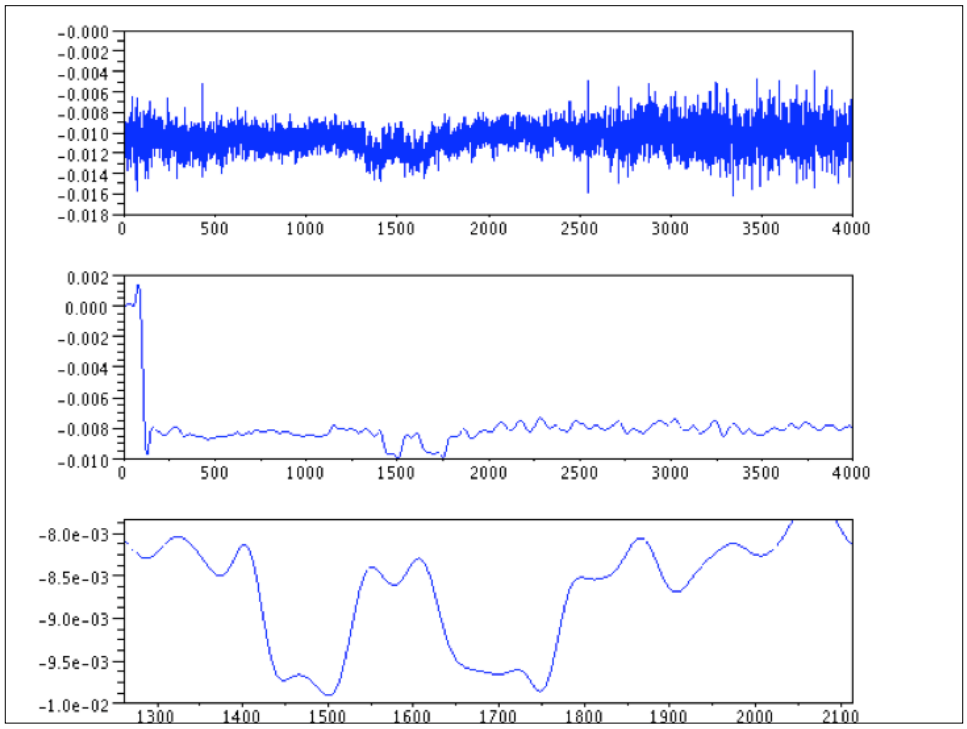
Relatively simple equipment can tap power lines to intercept what is being typed on nearby keyboards.

1. Unshielded wires in keyboard cables leak keystroke signals into the cable ground.

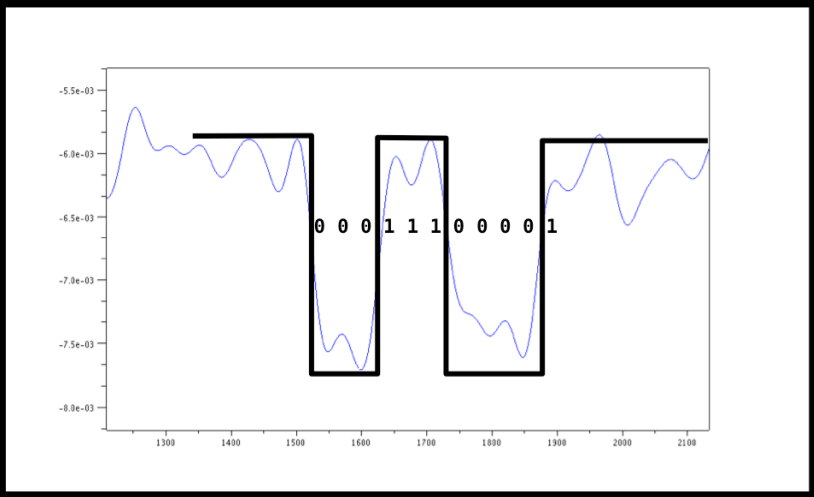
2. The signals continue along the ground wire of the electrical service feeding the PC.

3. Measuring voltage shifts across an extension of the electric-system ground reveals what keys are being struck.



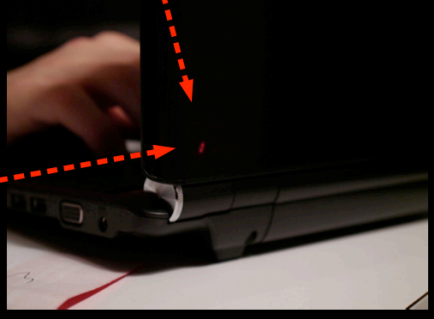


- | 0 | 00111000 | 0 | 1 | = letter 'a'



http://www.fickr.com/photos/thefineed1/68647955 http://creativecommons.org/licenses/by-nc-sa/2.0

Reflective Plastic Case



PWNED!

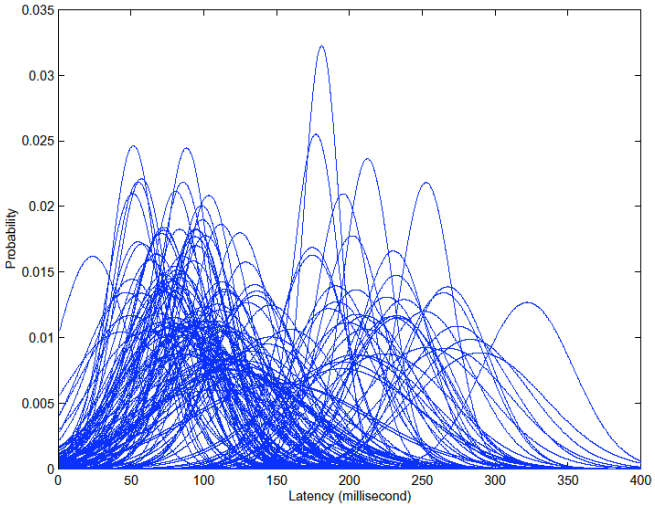
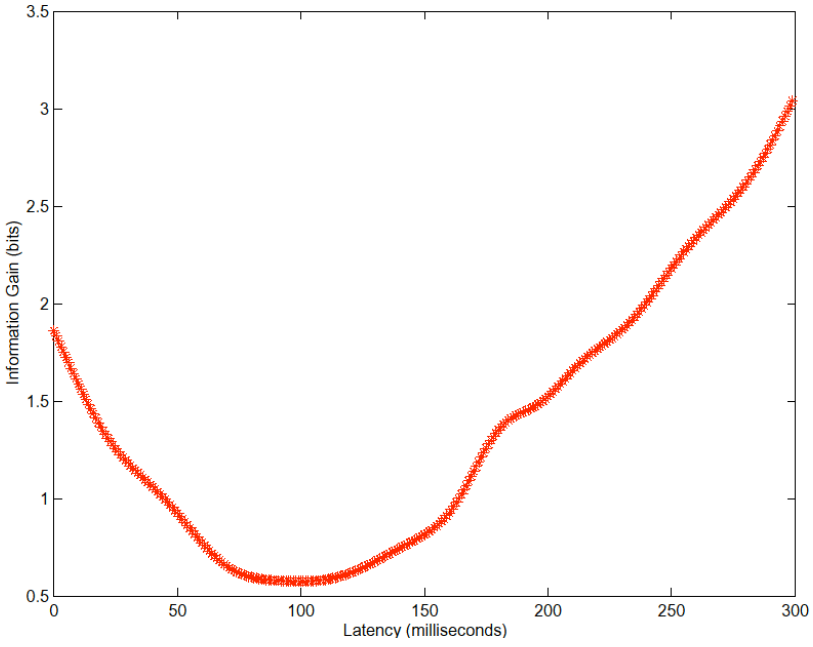
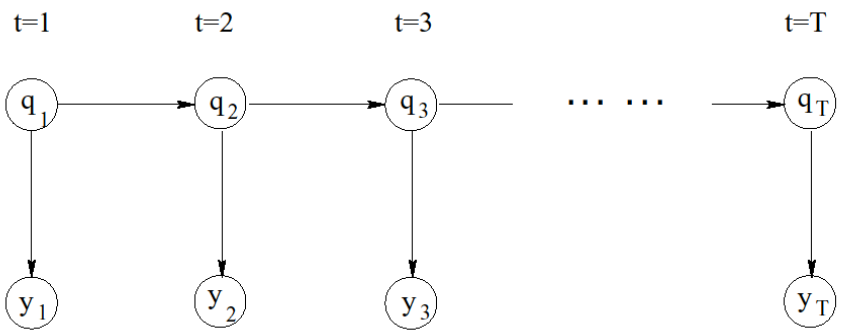


Figure 5: Estimated Gaussian distributions of all 142 character pairs collected from a user.





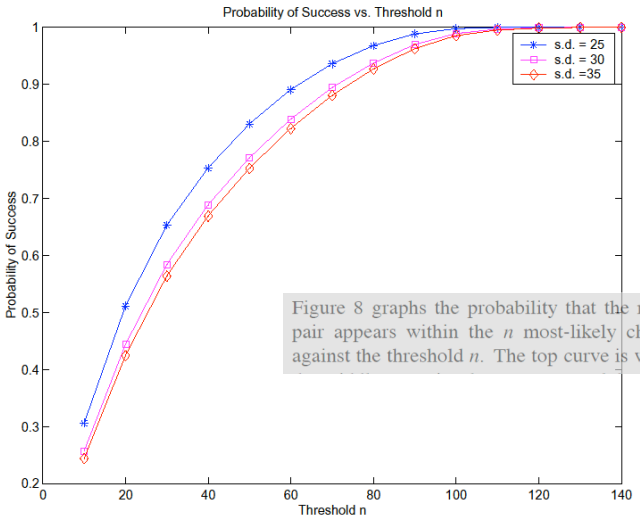


Figure 8 graphs the probability that the real character pair appears within the n most-likely character pairs against the threshold n. The top curve is when $\sigma = 25$,

Figure 8: The probability that the n-Viterbi algorithm outputs the correct password before the first n guesses, graphed as a function of n.

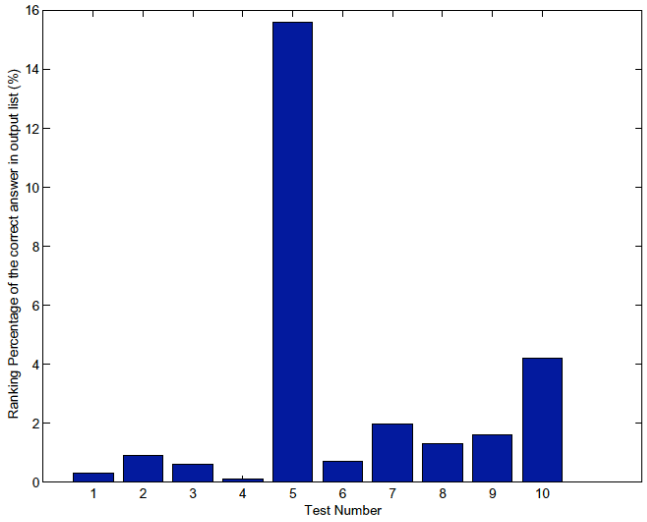
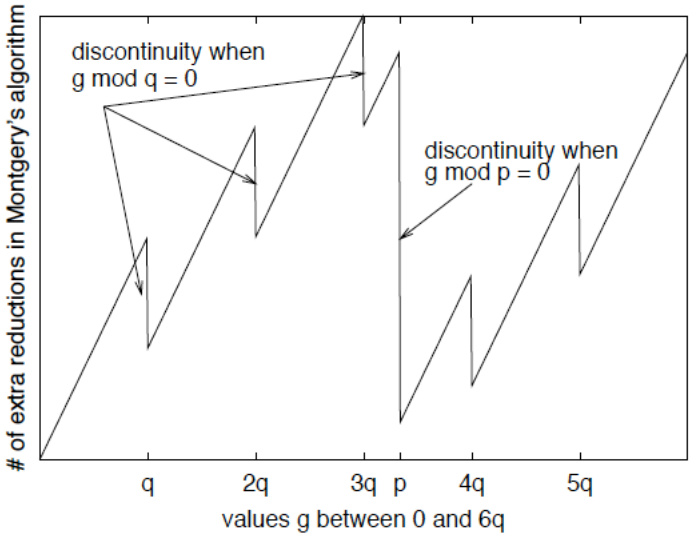
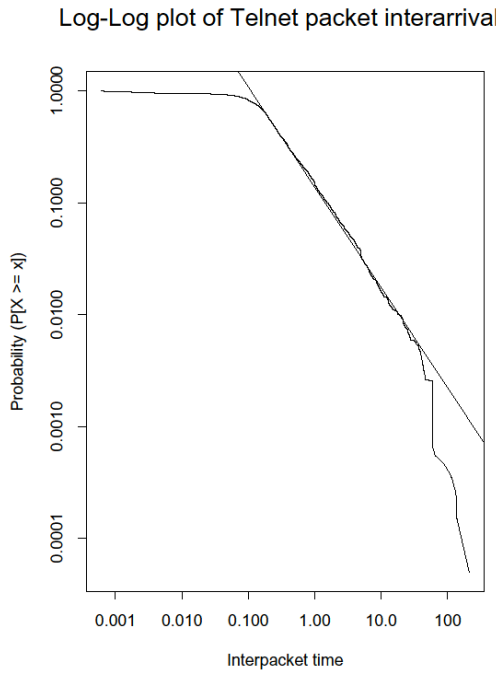


Figure 10: The percentage of the password space tried by Herbivore in 10 tests before finding the right password.

Training Set	Test Set	Test Cases				
		Password 1	Password 2	Password 3	Password 4	Password 5
User 1	User 1	15.6%	0.7%	2.0%	1.3%	1.6%
User 1	User 2	62.3%	15.2%	7.0%	14.8%	0.3%
User 1	User 3	6.4%	N/A	1.8%	3.1%	4.2%
User 1	User 4	1.9%	31.4%	1.1%	0.1%	28.8%
User 2	User 1	4.9%	1.3%	1.6%	12.3%	3.1%
User 2	User 2	30.8%	15.0%	2.8%	3.7%	2.9%
User 2	User 3	4.7%	N/A	5.3%	6.7%	38.4%
User 2	User 4	0.7%	16.8%	3.9%	0.6%	5.4%

Table 1: Success rates for password inference with multiple users. The numbers are the percentage of the search space the attacker has to search before he finds the right password.


discontinuity when
g mod q = 0
discontinuity when
g mod p = 0
# of extra reductions in Montgery's algorithm
q
2q
3q
p
4q
5q
values g between 0 and 6q


Log-Log plot of Telnet packet interarrivals
Probability (P[X >= x])
1.0000
0.1000
0.0100
0.0010
0.0001
0.001
0.010
0.100
1.00
10.0
100
Interpacket time