3 Assignment 3 (11 Points)

Hinweis:	Abgabe in $\{2, 3, 4\}$-er Gruppen.
Abgabe:	**13.05.2017, 23.59**
Email:	Betreff “[Compsec] Ex3” (bitte nur .pdf oder .txt, kein .doc, .jpeg, etc) Source code: bitte inkl. `signify` Signatur

Exercise 5 (Markov-Generator (**5 Points**))**.**
Consider the following sample of 4-digit PINs sampled from a PIN-database.

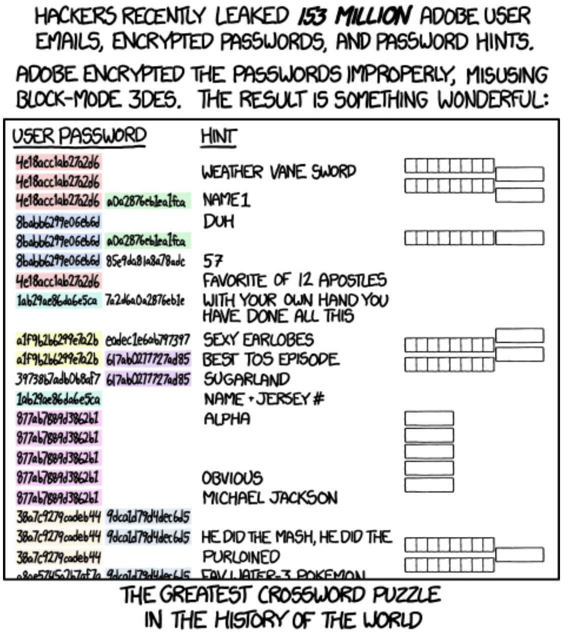
1331
2303
1301
2320
1312
1330
1203
1033
2332
2323

1. Construct a first-order Markov generator for this sample
2. Construct a second-order Markov generator for this sample
3. Give one 4-digit PIN number that is generated by your first-order Markov generator but not by your second-order generator and calculate it’s probability.

Note: You may want to report the probabilities in a table rather than a graph.

Exercise 6 (Bad Password Practice (**1+2 Points**))**.**

1. Visit `http://zed0.co.uk/crossword/` and solve one crossword.
2. What did Adobe do wrong? **Hint: (source:** `http://xkcd.com/1286/`**)**


HACKERS RECENTLY LEAKED 153 MILLION ADOBE USER EMAILS, ENCRYPTED PASSWORDS, AND PASSWORD HINTS.
ADOBE ENCRYPTED THE PASSWORDS IMPROPERLY, MISUSING BLOCK-MODE 3DES. THE RESULT IS SOMETHING WONDERFUL:
THE GREATEST CROSSWORD PUZZLE IN THE HISTORY OF THE WORLD

USER PASSWORD		HINT
4e18acc1ab27a2d6		WEATHER VANE SWORD
4e18acc1ab27a2d6		
4e18acc1ab27a2d6	a0a2876eb1ea1fca	NAME1
8babb6299e06eb6d		DUH
8babb6299e06eb6d	a0a2876eb1ea1fca	
8babb6299e06eb6d	85e9da81a8a78adc	57
4e18acc1ab27a2d6		FAVORITE OF 12 APOSTLES
1ab29ae86da6e5ca	7a2d6a0a2876eb1e	WITH YOUR OWN HAND YOU HAVE DONE ALL THIS
a1f96266299e7a2b	eadec1e6ab797397	SEXY EARLOBES
a1f96266299e7a2b	617ab0277727ad85	BEST TOS EPISODE
3973867adb068af7	617ab0277727ad85	SUGARLAND
1ab29ae86da6e5ca		NAME + JERSEY #
877ab7889d3862b1		ALPHA
877ab7889d3862b1		
877ab7889d3862b1		
877ab7889d3862b1		OBVIOUS
877ab7889d3862b1		MICHAEL JACKSON
38a7c9279cadeb44	9dca1d79d4dec6d5	
38a7c9279cadeb44	9dca1d79d4dec6d5	HE DID THE MASH, HE DID THE
38a7c9279cadeb44		PURLOINED
a8ae5745a2b7af7a	9dca1d79d4dec6d5	FAV WATER-3 POKEMON

Exercise 7 (Randomized Response (**2+1 Points**)).
Consider the following randomized response protocol for N participants. Each participant has a secret bit $r_i \in \{0, 1\}$ that he/she wants to keep secret and the goal is to estimate $\sum_{i=1}^{N} r_i$ (i.e. the total number of r_i with $r_i = 1$). When asked for a reply, each participants privately flips a bit b_i with $\Pr[b_i = 1] = 0.25$ and replies with $r'_i := r_i \oplus b_i$.

1. Show how you can estimate $\sum_{i=1}^{N} r_i$ when given $\sum_{i=1}^{N} r'_i$. **Hint:** model r_i, r'_i and b_i as random variables over a probability space. You may then use the fact that
$$E\left[\sum_{i=1}^{N} X_i\right] = \sum_{i=1}^{N} E\left[X_i\right]$$
holds for the sum of the expected values E of random variables X_i.

2. Show that this protocol (interpreted as randomized algorithm) is $(\log 3, 0)$-differentially private. **Hint:** Show that for arbitrary i it is
$$\Pr[R'_i = b \mid R_i = 1] \leq \exp(\log(3)) \cdot \Pr[R'_i = 1 - b \mid R_i = 0] + 0,$$
for $b \in \{0, 1\}$.

Exercise 8 (Keeping your systems secure (**Bonus: 1 Points**)).
Are there any new vulnerabilities for your Debian or OpenBSD system since last week (29.04.2016 at 23.59)? If so: state one, name the programming mistake, decide if you are affected or not, and report if there are any known work-arounds or patches.