IV054 Coding, Cryptography and Cryptographic Protocols
2017 - Exercises X.

1. Consider the coin-flipping by telephone protocol (*Protocol 2* from the lecture). Let $p = 11$, $q = 23$ and $x = 52$. Show computation steps in detail.
2. Alice and Bob have a boolean function $f : \{0,1\} \times \{0,1\} \to \{0,1\}$ known to both of them. Show that if f is not a constant function there is no protocol that lets them perfectly evaluate $f(a,b)$ on all respective secret inputs a and b without neither party obtaining any information about the other party's secret.
3. Consider 30 combination padlocks where Victor knows the combinations for all of them. Give a protocol that allows Peggy to prove to Victor that she knows the combination for at least one of the padlocks without revealing which one.
4. Consider the following commitment scheme, with the following public information: p a large prime, g a generator of $\mathbb{Z}_p^*$ and $h = g^k \bmod p$ with $0 < k < p-1$ a random integer not known to any party. The commitment function is

$$\text{commit}(r,x) = (g^r \bmod p, h^{r+x} \bmod p),$$

   where x is the committed bit and $0 < r < p$ a random integer.

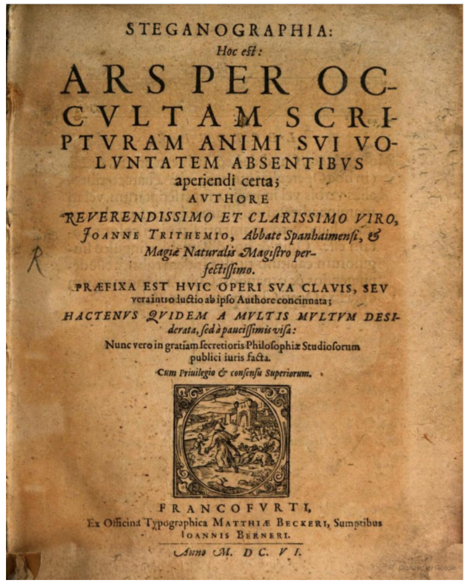
   (a) Find a reveal phase for this protocol.

   (b) Discuss the binding and hiding properties of this protocol. Are they computationally/information-theoretically secure?

   (c) What happens if Bob (the receiver) knows $\log_g(h)$?
5. Alice and Bob are using the *Bit commitment scheme II* from the lecture slides, but Bob does not trust Alice and wants her to commit her bit b twice using the same α but different x_0 and x_1 to create commitments $f_0 = f(b, x_0)$ and $f_1 = f(b, x_1)$. Bob is also lazy and instead of opening both of the commitments separately and checking if his received commitments f_0 and f_1 are equal to $f(b, x_0)$ and $f(b, x_1)$, respectively, he just checks whether $f(b, x_0 + x_1) = f_0 \cdot f_1$. Will this protocol open the bit commitment correctly?
6. Show that the following variants of oblivious transfer are equivalent:
   - *Rabin oblivious transfer:* Alice transmits a bit b to Bob, who receives either b or $\perp$ (indicating that the bit was not received), each case with probability $\frac{1}{2}$. Alice does not know which is the case.
   - 1-*out-of-*2 *oblivious transfer:* Alice has two bits b_0 and b_1. Bob chooses $c \in \{0,1\}$, learns b_c but not b_{1-c}. Alice does not learn c.
   - 1-*out-of-k oblivious transfer:* Alice has k bits $b_1, \ldots, b_k$. Bob chooses $c \in \{1, \ldots, k\}$, learns b_c but none of the others. Alice does not learn c.
7. Victor is color-blind and cannot distinguish between colors at all. Peggy who can see colors has two apples, one green and one red, but otherwise identical. Design a zero-knowledge protocol that allows Peggy to convince Victor that the apples have different colors.

More on next page >>>

8. *Bonus exercise*
   This is the title page of a book called *Steganographia*.


STEGANOGRAPHIA:
Hoc est:
ARS PER OC-
CVLTAM SCRI-
PTVRAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
JOANNE TRITHEMIO, *Abbate Spanhaimensi, &*
Magiæ Naturalis Magistro per-
fectissimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
vera introductio ab ipso Authore concinnata;
HACTENVS QVIDEM A MVLTIS MVLTVM DESI-
derata, sed à paucissimis visa:
Nunc vero in gratiam secretioris Philosophiæ Studiosorum
publici iuris facta.
Cum Priuilegio & consensu Superiorum.

FRANCOFVRTI,
Ex Officina Typographica MATTHIÆ BECKERI, Sumptibus
IOANNIS BERNERI.
Anno M. DC. VI.

You can find the copy of this picture in the study materials.