Introduction to Modern Cryptography
Class Exercises #1

University of Amsterdam, Master of Logic, 2014
Lecturer: Christian Schaffner
TA: Malvin Gattinger

Thursday, 4 September 2014

Class Exercises (to be solved during exercise class)

1. Questions about the video lectures:
   (a) Name some cryptographic primitives and use cases.
   (b) What is modern about Modern Cryptography?
   (c) What is the keyspace for the substitution, Vigener and the one-time pad ciphers?
   (d) Give examples for deterministic and randomized algorithms.
   (e) Why could the birthday paradox be relevant in Cryptography?

2. State the contrapositive of the following statements:
   (a) If it rains, the trees get wet.
   (b) If the car drives, its fuel tank is not empty.
   (c) If p is a prime, then $p = 2$ or p is odd.
   (d) If assumption X holds, protocol Y is secure.
   (e) If you can factorize efficiently, the RSA protocol is insecure.

3. Let the probability that a news article contains the word *president* be 20%. The probability that it contains the word *president* if it already contains the word *Obama* is 35%. The probability that it contains the word *president* if it does not contain the word *Obama* is 5%.

   Under these assumptions, what is the probability that a news article contains the word *Obama*?

4. **Probability theory** Let E_1 and E_2 be probability events. Then, $E_1 \wedge E_2$ denotes their conjunction, i.e. $E_1 \wedge E_2$ is the event that *both* E_1 and E_2 occur. The *conditional probability of* E_1 *given* E_2, denoted $\Pr[E_1|E_2]$ is defined as

   $$\Pr[E_1|E_2] := \frac{\Pr[E_1 \wedge E_2]}{\Pr[E_2]}$$

   as long as $\Pr[E_2] \neq 0$. Prove Bayes' theorem.

   Theorem 1 (Bayes' theorem) *Let E_1 and E_2 be probability events with $Pr[E_2] \neq 0$. Then,*

   $$Pr[E_1|E_2] = \frac{Pr[E_1] \cdot Pr[E_2|E_1]}{Pr[E_2]} .$$