Introduction to Modern Cryptography
Class Exercises #2

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

Thursday, 11 September 2014

Class Exercises (to be solved during exercise class)

1. (a) Think of a PPT algorithm for picking a uniformly random key from the key space $\mathcal{K}$, where $|\mathcal{K}| = 2^n$ for some $n \in \mathbb{N}$.
   (b) Explain why no PPT algorithm exists if $|\mathcal{K}|$ is not a power of two. How can you pick a uniform key in that case?

2. Let $a > 1$ be a real constant. Show that $\frac{1}{a^n}$ is a negligible function.

3. Prove whether or not each of the following functions is negligible.
   (a) 0.80^n
   (b) $\frac{1}{2^{80}n}$
   (c) $\frac{1}{2^{80n}}$
   (d) $2^{-\log_2(n^{80})}$

4. Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a pseudorandom generator. Show the existence of an exponential-time distinguisher D that distinguishes well between a random $r \leftarrow \{0,1\}^{2n}$ and a pseudo-random string $G(s)$ for $s \leftarrow \{0,1\}^n$.

5. Archaeologists found the following encryption table — unfortunately it is not complete.

	$>$	$\vee$	$<$	$\wedge$
$\bullet$			$<$	$\wedge$
$\leftrightarrows$	$<$	$\wedge$	$>$	
$\circlearrowleft$	$\wedge$	$>$		
$\circlearrowright$				

   On another papyrus it is explained that this encryption was used during war. The movements "left", "right", "attack" and "withdrawal" were represented by $\mathcal{M} = \{<, >, \wedge, \vee\}$. The keyspace was $\mathcal{K} = \{\bullet, \leftrightarrows, \circlearrowleft, \circlearrowright\}$. Ciphertext and plaintext used the same alphabet, i.e. $\mathcal{C} = \mathcal{M}$.

   The key was picked by tossing a coin twice. For every transmission a new key was used.

   Complete the table to form a perfectly secure encryption scheme. Prove the perfect security, using Shannon's theorem.

6. Exercise 2.2 from [KL]: Prove or refute: For every encryption scheme that is perfectly secret, it holds that for every distribution over the message space $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$:

$$\Pr[M = m \mid C = c] = \Pr[M = m' \mid C = c] \ .$$

7. Exercise 2.5 from [KL]: Prove or refute: Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

8. Exercise 2.13. from [KL]. Let $0 < \varepsilon < 1$. An encryption scheme is called ε-perfectly secure, if for any distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any $c \in \mathcal{C}$, it holds that

$$|\Pr[M = m \mid C = c] - \Pr[M = m]| < \varepsilon \, .$$

   Prove the following generalisation of Theorem 2.7:

   Theorem 1 *Let $0 < \varepsilon < 1$ and let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an ε-perfectly secret encryption scheme over a message space $\mathcal{M}$. Then $|\mathcal{K}| \geq |\mathcal{M}|$.*