MTAT.07.003 Cryptology II
Spring 2009 / Exercise Session II

1. There are many ways how to attack a standard e-banking system. First, an attacker can distribute malware that logs all kinds of passwords. Secondly, an attacker can send out forged e-mails that instruct bank customers to send passwords to a certain mail account. Thirdly, an attacker can attack the underlying cryptographic protection mechanism. When the attacker has a control over the account, he or she has to withdraw the money through an auxiliary account belonging to a mule. This poses a risk as mules do not always deliver the money to attacker's account.

   Compute a success probabilities of all attack scenarios and find the one with highest expected gain, given only some estimates of conditional probabilities. Namely, let $\mathsf{Malware}$, $\mathsf{Phishing}$ and $\mathsf{CryptoBreak}$ denote success in the first attack step. Let Detect denote the event that an unauthorised bank transfer or the attack itself is detected. Finally, let Cheat denote the event that mule cheats and the attacker does not get the money. Then

$$
\begin{aligned}
\Pr\left[\mathsf{Malware}\right] &= 10^{-3} & \Pr\left[\mathsf{Detect}|\mathsf{Malware}\right] &= 10^{-4}\\
\Pr\left[\mathsf{Phishing}\right] &= 10^{-2} & \Pr\left[\mathsf{Detect}|\mathsf{Phishing}\right] &= 1\\
\Pr\left[\mathsf{CryptoBreak}\right] &= 10^{-27} & \Pr\left[\mathsf{Detect}|\mathsf{CryptoBreak}\right] &= 0\\
\Pr\left[\mathsf{Detect}|\mathsf{Draw\ 100}\right] &= 10^{-2} & \Pr\left[\mathsf{Cheat}|\mathsf{Draw\ 100}\right] &= 0\\
\Pr\left[\mathsf{Detect}|\mathsf{Draw\ 1000}\right] &= 10^{-1} & \Pr\left[\mathsf{Cheat}|\mathsf{Draw\ 1000}\right] &= 10^{-1}\\
\Pr\left[\mathsf{Detect}|\mathsf{Draw\ 10000}\right] &= 1 & \Pr\left[\mathsf{Cheat}|\mathsf{Draw\ 1000}\right] &= 10^{-2}
\end{aligned}
$$

   What is probability that the corresponding attacks remain unnoticed?

2. Bob has a biased coin such that in each throw the probability of getting a tail is α. Additionally, assume that all coin tosses are independent.

   (a) How many throws are needed on average to see the first tail?

   (b) How many throws are needed on average to see k tails?

   Now consider a scenario, where Bob must see at least two tails to succeed.

   (c) How many throws are needed to succeed with probability at least $\frac{1}{2}$? Give a simple and safe upper bound on the number of throws.

   (d) Show that Bob must make at least $\Omega(\frac{1}{\alpha})$ throws to achieve constant success probability in the process $\alpha \to 0$.

   (e) How many throws are needed to achieve exponentially small failure probability ε?

   Hints: Use Markov's and Chebyshev's inequalities. Answers of the questions (c) and (e) are tightly connected.

3. A cryptosystem is a triple of algorithms $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ such that the equality $\mathcal{D}(\mathcal{E}(m, k), k) = m$ holds for all messages $m \in \mathcal{M}$ and keys $k \leftarrow \mathcal{K}$. Cryptosystem is perfectly secure if a ciphertext c reveals nothing about the corresponding message m, i.e., $\Pr[m|c] = \Pr[m]$.

   (a) Prove that cryptosystem is perfectly secure only if $H(m|c) = H(m)$. What about the implication to the other direction?

   (b) Show that $H(k, m, c) \geq H(m|c) + H(c)$. For which enciphering algorithms does the equality $H(k, m, c) = H(m|c) + H(c)$ hold?

   (c) Show that $H(k, m, c) = H(k) + H(c|k)$. Conclude that cryptosystem is perfectly secure only if $H(k) \geq H(m)$.

   (d) Show that $H(k|c) = H(m) + H(k) + H(c|m, k) - H(c)$. What does the result mean in practise?

4. Estimate how much time is needed to break the following three file encryption methods without using cipher-specific attacks.

   (a) The file is encrypted with 128-bit AES cipher and the key is stored in a special file that is protected with a password. Namely, the key is encrypted with another key that is derived form the password.

   (b) The file is encrypted with old 56-bit DES cipher and the key is stored in the special file that is encrypted with a public key. The corresponding secret key is stored in the ID card.

   (c) The file is encrypted with 80-bit IDEA cipher and the key is stored in the special file that is encrypted with a public key. The corresponding secret key is stored in the TPM chip.

5. Let $\mathcal{X}_0$ be a uniform distribution over $\mathbb{Z}_{16}$ and let $\mathcal{X}_1$ be a uniform distribution over $\{0, 2, 4, 6, 8, 10, 12, 14\}$.

   (a) What is the statistical difference between $\mathcal{X}_0$ and $\mathcal{X}_1$?

   (b) Find an distinguishing strategy $\mathcal{A}$ that minimises the ratio of false positives $\beta(\mathcal{A})$ and achieves false negative rate $\alpha(\mathcal{A}) = 0\%$.

   (c) Find an distinguishing strategy $\mathcal{A}$ that minimises the ratio of false positives $\beta(\mathcal{A})$ and achieves false negative rate $\alpha(\mathcal{A}) \leq 50\%$.

   (d) Generalise the distinguishing strategy and find minimal ratio of false positives $\beta(\mathcal{A})$ for all bounds $\alpha(\mathcal{A}) \leq \alpha_0$.

6. Normally, it is impossible to compute computational distance between two distributions directly since the number of potential distinguishing algorithms is humongous. However, for really small time-bounds it can be done. Here, we assume that all distinguishers $\mathcal{A} : \mathbb{Z}_{16} \to \{0, 1\}$ are implemented as Boolean circuits consisting of NOT, AND and OR gates and the corresponding time-complexity is just the number of logic gates. For example, $\mathcal{A}(x_3x_2x_1x_0) = x_1$ has time-complexity 0 and $\mathcal{A}(x_3x_2x_1x_0) = x_1 \vee \neg x_3 \wedge x_2$ has time-complexity 3.

(a) Let $\mathcal{X}_0$ be a uniform distribution over $\mathbb{Z}_{16}$ and let $\mathcal{X}_1$ be a uniform distribution over $\{0, 2, 4, 6, 8, 10, 12, 14\}$. What is $\mathsf{cd}_x^1(\mathcal{X}_0, \mathcal{X}_1)$?

(b) Find a uniform distribution $\mathcal{X}_2$ over some 8 element set such that $\mathsf{cd}_x^1(\mathcal{X}_0, \mathcal{X}_2)$ is minimal. Compute $\mathsf{cd}_x^2(\mathcal{X}_0, \mathcal{X}_2)$ and $\mathsf{cd}_x^3(\mathcal{X}_0, \mathcal{X}_2)$.

(c) Find a uniform distribution $\mathcal{X}_3$ over some 8 element set such that $\mathsf{cd}_x^1(\mathcal{X}_0, \mathcal{X}_3) + \mathsf{cd}_x^1(\mathcal{X}_0, \mathcal{X}_3)$ is minimal.

(d) Estimate for which value of t the distances $\mathsf{cd}_x^t(\mathcal{X}_0, \mathcal{X}_1)$ and $\mathsf{sd}_x(\mathcal{X}_0, \mathcal{X}_1)$ coincide for all distributions over $\mathbb{Z}_{16}$.

($\star$) Let the time-complexity of distinguishing algorithms be defined as in the previous exercise. Find disjoint distributions $\mathcal{X}_0$ and $\mathcal{X}_1$ over $\mathbb{Z}_{256}$ such that their computational distance is minimal. Tabulate the results for time-bounds $0, 1, \ldots, 16$. More precisely, find the optimal distribution pair for each time-bound and their computational distance for all time-bounds.