Problem Set 4
Cryptographic Hash Functions
(Summer Term 2017)

Bauhaus-Universität Weimar, Chair of Media Security
Prof. Dr. Stefan Lucks, Eik List
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching/`

Due Date: 30 May 2017, 1:30 PM, via email to `eik.list(at)uni-weimar.de`.

Goal of this Problem Set: Understanding differential cryptanalysis, CVHP, and the security of MDC2.

Task 1 – MD4 (4 Credits)
Recap differential cryptanalysis, e.g., from the end of this problem set. Recap Slides 103 pp. from Chapter 5..

a) Show and explain the differential characteristic for the second example where $X_i = X'_i$, for $i \notin \{0, 1\}$ over Steps 3-32. Compute the probability of this characteristic when $X_0 \oplus X'_0 = 2^j$ and $X_1 \oplus X'_1 = 2^{(j+3) \bmod 32}$ for arbitrary $j \in \{0, \ldots, 31\}$ *(Hint: Draw the construction as first step).*

b) What is the specific probability if $j = 28$?

Task 2 – MD4 (4 Credits)
Consider the attacks on MD4 from Chapter 5 of the lecture. Find a differential characteristic different from that in Task 1 with probability $\geq 2^{-6}$ over as many steps of MD4 as you can, but over at least 30 steps.

Task 3 – CVHP (3 Credits)
Let p be a Sophie-Germain prime, i.e., $q = (p-1)/2$ is also prime, with $p, q > 3$. Let g be a generator of $\mathbb{Z}_p^*$ and $b \twoheadleftarrow \mathbb{Z}_p$. Then, the Chaum-van-Heijst-Pfitzmann hash function $\mathrm{CVHP} : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{Z}_p$ is defined as

$$\mathrm{CVHP}_{g,b}(x, y) := g^x \cdot b^y \bmod p.$$

The collision resistance of CVHP can be reduced to the discrete-logarithm problem of finding $\log_g(b)$ in $\mathbb{Z}_p$; i.e., given a collision $\mathrm{CVHP}(x, y) = \mathrm{CVHP}(x', y')$ for distinct $(x, y), (x', y') \in \mathbb{Z}_q^2$, one can efficiently compute $\log_g(b)$. In this task, you shall apply the inverse. You can obtain more information, e.g. from Section 7.4 of Crépeau's book. Let $q = 97001$, $g = 2$, and let $\log_g(b) = 9435$. Compute a collision for $\mathrm{CVHP}_{g,b}$ and explain your solution.

Task 4 – Simplified MDC2 (3+3 Credits)
The compression function $F : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is defined as follows:

$$(G_i, H_i) := F(G_{i-1}, H_{i-1}, M_i) := (E_{G_{i-1}}(M_i) \oplus M_i, E_{H_{i-1}}(M_i) \oplus M_i).$$

The hash function $\mathcal{H}$ then fixes (G_0, H_0) with $G_0, H_0 \neq 0^n$. We concentrate on single-block messages for simplicity, i.e., (G_1, H_1) is the hash value for a message M_1.

a) Analyze the collision, preimage, and second-preimage security of F.

b) Analyze the collision, preimage, and second-preimage security of $\mathcal{H}$ for single-block messages.

Describe an algorithm against the respective construction with the lowest possible complexity *(Hint: Draw the construction as your first step).*

Differential Cryptanalysis in a Nutshell: Assume $E(X) := F_r(F_{r-1}(\cdots F_1(X)))$ is an iterated cryptographic transform, i.e., a round-based transform that consists of r iterations of a round function $F_i : \{0,1\}^n \to \{0,1\}^n$. For n-bit strings $X, X' \in \{0,1\}^n$, we define their XOR difference by $\Delta := X \oplus X'$, and their additive difference by $\Delta := (X - X') \bmod 2^n$. In the following, we use XOR differences if not stated otherwise.

A *differential* $\Delta X \xrightarrow{F} \Delta Y$ is a mapping of inputs X, X' with $X \oplus X' = \Delta X$ to outputs Y, Y' with $Y \oplus Y' = \Delta Y$ over a function F. An *r-round differential characteristic* is a sequence of differences: $(\Delta_0, \Delta_1, \ldots, \Delta_r)$, where Δ_i denotes the difference after Round i. We denote by $\Pr_X[\Delta X \xrightarrow{F} \Delta Y]$ the *differential probability*. Under the Markov-cipher assumption and the hypothesis of stochastic independence [1], we assume that it holds for a given differential characteristic over E:

$$\Pr\left[(\Delta_0, \Delta_1, \ldots, \Delta_r)\right] = \prod_{i=1}^{r} \Pr\left[\Delta_{i-1} \xrightarrow{F_i} \Delta_i\right] \text{ for all } i \text{ and all } \Delta_i.$$

References

[1] Xuejia Lai, James L. Massey, and Sean Murphy. Markov Ciphers and Differential Cryptanalysis. In Donald W. Davies, editor, EUROCRYPT, volume 547 of Lecture Notes in Computer Science, pages 17–38. Springer, 1991.