Problem Set 4
Cryptographic Hash Functions
(Summer Term 2019)

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

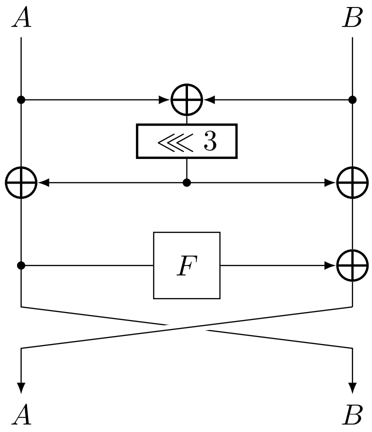
Due Date: 6 June 2019, 11:00 AM, via email to `jannis.bossert(at)uni-weimar.de`.

Goal of this Problem Set: Understanding differential cryptanalysis and the security of Weimar-DM.

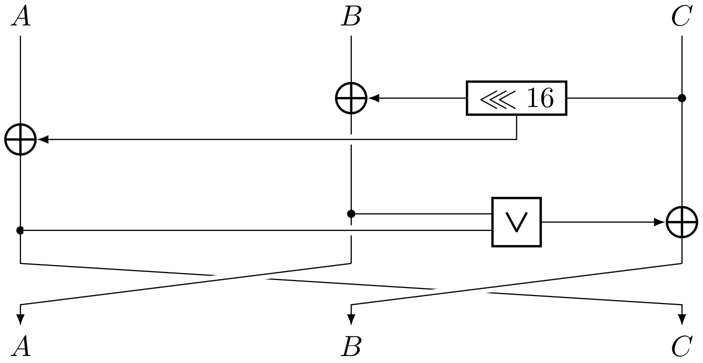
Task 1 – Differential Cryptanalysis Recap (1 + 2 Credits)

Recap differential cryptanalysis, e.g., from the end of this problem set. The function F in the constructions below fulfills the property that $\Pr[\alpha \to \beta] = 2^{-5}$, for arbitrary α, β. Your task is to find a differential characteristic over as many rounds as possible with a $\Pr[\Delta_{in} \to \Delta_{out}] \geq 2^{-10}$ for both constructions. Both constructions work on 32-bit words.

a)



b)



Task 2 – MD4 (4 Credits)

Recap differential cryptanalysis, e.g., from the end of this problem set. Recap Slides 103 pp. from Chapter 5.

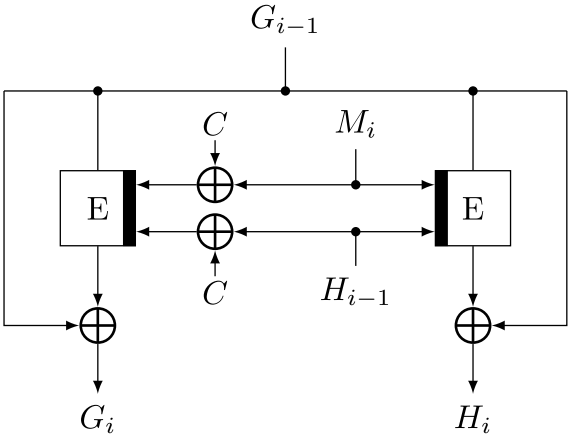
a) Show and explain the differential characteristic for the second example where $X_i = X_i'$, for $i \notin \{0, 1\}$ over Steps 3-32. Compute the probability of this characteristic when $X_0 \oplus X_0' = 2^j$ and $X_1 \oplus X_1' = 2^{(j+3) \bmod 32}$ for arbitrary $j \in \{0, \ldots, 31\}$ *(Hint: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

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

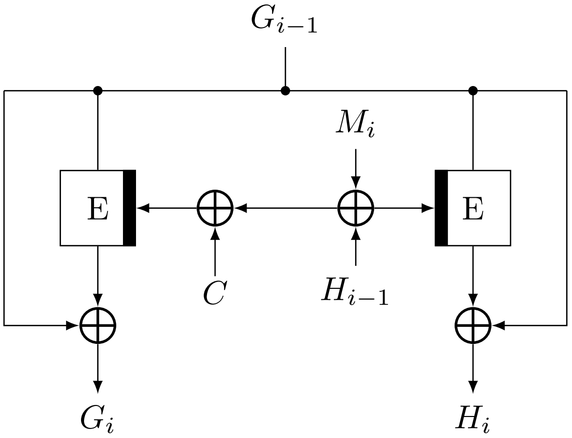
Task 3 – MD4 (4 Credits)
Consider the attacks on MD4 from Chapter 5 of the lecture. Find a differential characteristic different from that in Task 1 with probability $\geq 2^{-6}$ over as many steps of MD4 as you can, but over at least 30 steps.

Task 4 – Simplified Weimar-DM (2+2+3 Credits)
In the following you are asked to analyze three variations of Weimar-DM and their impacts on the collision, preimage and second-preimage security.

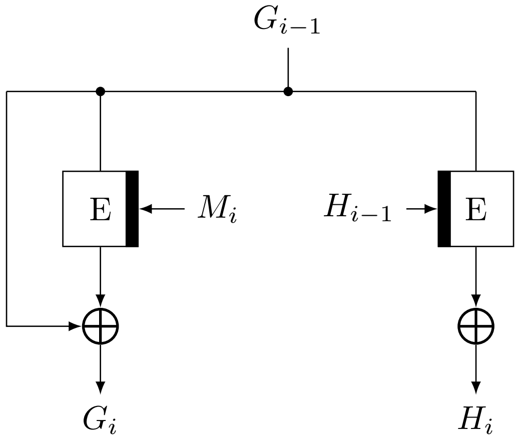
a) How would the choice of $c = 0$ affect the three security measures.



b) In this variation the block cipher uses a key of length n. The left encryption key is $c \oplus M_i \oplus H_{i-1}$ and the right encryption key is $M_i \oplus H_{i-1}$.



c) Here, we eliminate the feed-forward on the right side of Weimar-DM. Also the left encryption key is M_i and the right encryption key is H_{i-1}.



Differential Cryptanalysis in a Nutshell: Assume $E(X) \overset{\text{def}}{=} F_r(F_{r-1}(\cdots F_1(X)))$ is an iterated cryptographic transform, i.e., a round-based transform that consists of r iterations of a round function $F_i : \{0,1\}^n \rightarrow \{0,1\}^n$. For n-bit strings $X, X' \in \{0,1\}^n$, we define their XOR difference by $\Delta \overset{\text{def}}{=} X \oplus X'$, and their additive difference by $\Delta \overset{\text{def}}{=} (X - X') \bmod 2^n$. 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.