RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 9 / 11. Dezember 2011

AUFGABE 1:
Zeigen Sie, dass 3 ein Erzeuger der multiplikativen Gruppe $\mathbb{Z}^*_{65537}$ ist. Was ist $\text{dlog}_3(19) \bmod 2$?
Anmerkung: $65537 = 2^{16} + 1$ ist prim.

AUFGABE 2:
Bestimmen Sie mit Hilfe des Pohlig-Hellman Algorithmus den diskreten Logarithmus von 59 zur Basis 3 in der multiplikativen Gruppe $\mathbb{Z}^*_{152}$, sofern existent. $(152 = 8 \cdot 19)$
Bestimmen Sie mit Hilfe des Pohlig-Hellman Algorithmus den diskreten Logarithmus von 39 zur Basis 3 in der multiplikativen Gruppe $\mathbb{Z}^*_{85}$, sofern existent.

AUFGABE 3:
Sie werfen mit ihrem Freund Münzen. Wenn Sie das Ergebnis richtig vorhersagen, dürfen Sie die Münze behalten, andernfalls müssen Sie ihrem Freund den Einsatz auszahlen. Die Wahrscheinlichkeit, dass eine Münze auf der Kante landet sei $\frac{1}{50}$. Sie spielen das Spiel genau $n = 10.000$ mal. Ist dies ein faires Spiel? Schätzen Sie die Wahrscheinlichkeit, dass Sie ohne Verlust herausgehen nach oben ab. Benutzen Sie dazu einmal die Hoeffding Schranke und einmal die Chebycheff-Ungleichung. Wie viel besser ist die Hoeffding Schranke bei $n = 100.000$?

AUFGABE 4:
Faktorisieren sie $77 = (1001101) = pq$ mit Hilfe der partiellen Information $p =??1?$und $q = 1?1?$ nach dem Algorithmus aus der Vorlesung. (auf Hausübung verlegt)