

# 暗号理論レポート

平成 22 年 12 月 1 日

書式: 基本的に自由. ただし A4 の紙を用い表紙に氏名と学籍番号を明記.

提出先: 授業時間に安富に直接手渡ししか 1 月から WW7F 安富個研に設置予定の提出箱.

期限: 1 月 19 日 (水) まで

1. 有限集合  $\Sigma = \{0, 1, 2, 3\}$  上に 2 つの分布

$$\Pr_{\Sigma}(0) = \Pr_{\Sigma}(1) = \Pr_{\Sigma}(3) = \frac{1}{5}, \quad \Pr_{\Sigma}(2) = \frac{2}{5}$$

と

$$\Pr'_{\Sigma}(0) = \Pr'_{\Sigma}(1) = \Pr'_{\Sigma}(2) = \Pr'_{\Sigma}(3) = \frac{1}{4},$$

を考える.

$$\iota : \Sigma \times \Sigma \ni (m, n) \mapsto m + n \pmod{4} \in \Sigma$$

- (a)  $\mathcal{P} = \mathcal{K} = \mathcal{C} := \Sigma$ ,  $\Pr_{\mathcal{P}} := \Pr_{\Sigma}$ ,  $\Pr_{\mathcal{K}} := \Pr'_{\Sigma}$ ,  $E := \iota$ ,  $D := E^{-1}$  とするとき (対称) 暗号系  $(\mathcal{P}, \mathcal{K}, \mathcal{C}, D, E)$  が完全守秘性を持つ事を示せ.

- (b)  $\mathcal{P} = \mathcal{K} = \mathcal{C} := \Sigma^2$ ,  $\Pr_{\mathcal{P}} := \Pr_{\Sigma}^2$ ,  $\Pr_{\mathcal{K}} := \Pr_{\Sigma}^{\prime 2}$ ,  $E((m, n)) := (\iota(m), \iota(n))$ ,  $D := E^{-1}$  とするとき (対称) 暗号系  $(\mathcal{P}, \mathcal{K}, \mathcal{C}, D, E)$  が完全守秘性を持たない事を示せ.

2. (a)  $7^{100}$  の 3 による剰余を求めよ.(計算過程も書くこと)

- (b) 341 が 2 を底とした擬素数である事を示せ.

- (c) 561 がカーマイケル数であることを示せ.