情報セキュリティ（宮崎）　**レ ポ ー ト 課 題**　（平成 26 年 11 月 11 日）

レポート提出締切：１１月２１日（金）午後５時（厳守）
提出先：情報科学部３階 学部事務室 レポート箱

次の規格の DES 暗号を用いて、暗号化および復号の操作を行え。

（1）平文を学籍番号の下３桁の数字（０～２５５）とする。これを８ビットで２進数表示し、暗号化せよ。暗号文は０～２５５の数字（１０進数）で表すこと。
（例）１２ＪＫ０５８ → ５８（平文）→ ？（暗号文）

（2）（1）で得られた暗号文（０～２５５の数字）を８ビットで２進数表示し、復号せよ。（学籍番号の下３桁の数字にもどれば OK！）

DES 暗号の規格：

◆ 平文・暗号文： ８ビット
◆ DES の段数： ２段
◆ 鍵（K）： $b_1b_2b_3b_4b_5b_6b_7b_8b_9$ （９ビット）
◆ 鍵スケジュール部： 鍵（K）→ 副鍵（K1,K2）（４ビット×２）

副鍵 K1： $b_1b_2b_3b_4$

副鍵 K2： $b_5b_6b_7b_8$ （注）鍵 K の第 9 ビット b_9 は使用しない。

◆ f 関数 $f(R,K) = S(R \oplus K)$
（参考：講義スライド 又は 配付資料（図 2.3））
◆ Ｓ箱の入出力関係（１０進数表示）

入力	0	1	2	3	4	5	6	7
出力	１０	5	9	１２	6	3	１４	2

入力	8	9	１０	１１	１２	１３	１４	１５
出力	4	１５	0	１１	１３	7	8	1

◆ ９ビットの鍵（K）は生年月日（X 月 Y 日）から次の要領でつくるものとする。

X（１～１２）→ ２進数表示 $b_1b_2b_3b_4$ （４ビット）

Y（１～３１）→ ２進数表示 $b_5b_6b_7b_8b_9$ （５ビット）

（例）１１月３０日の場合、鍵（K）は １０１１１１１１０ となる。