國立成功大學
National Cheng Kung University

對稱式密碼系統 補充4

計網中心 網路與資訊安全組

李南逸

作業4

- 請破解AES加密器產生之密文
  - 請同學將學號最後一碼mod 5，依所得之餘數x，嘗試解出第x組金鑰
    - ■: 尚未得知的密碼

	密文	金鑰
X=0	2NHkjlDyk82JBke5q8CnMQZ1iiHID8QEst+/Ld6lWFMP5om XXh/1LnmrYKOD04idKfzfL+6C96391/iN7+X0eg==	$"■vXl■K■\/ {9Fp■
X=1	INNkAZHIpe5u9LvzhH24VyORcZQVDCFXzV6V/l9M7rpgqsk MxvaRbGwR2dZaxMDZ	0lOS■b] ■&N) ■w■@+
X=2	NnJyrVT80DxOU5jOxHdZ9NRlaLPRhaAUYANfaVACUeqcrP oXz5eeTs9m6X2fVJC9SJ+X03mu3zD/WTiUjwzIyg==	Bk■fom] ■H■ (J■'|,
X=3	89NEvN56VtNjo1w5x3whmFUOZOqTaRyoMnIrPjCGKUv5n7 kgGFHDmStzEgDFAU7QnZOK9MLeO/FW4etzIOhpKfOsw5x SD4Em72X1O2FRfaM=	2■? ■mYD;@■;x■v"i
X=4	FZp57a6p84EUNC7I/ENj4RhPZtryOJr4che9JbA8ng1eI8ZMT lsl8kzicBDqkOqkFj3lwC69KR2MeA8lscVlig==	|q■~k=■&?I$Fx■N■

作業4

- 加密模式： ECB mode
- 演算法padding方式 : zeropadding
- 演算法運算時使用的編碼格式 : utf-8
- 先將密文從base64編碼格式轉成utf-8格式進行破解，最後再轉成字串查看明文結果
- 範例：金鑰是123456789 ，明文是security，輸出密文是

  pKjVPv28yVMn5cRXeUNYpg==

- 繳交
  - 1. Pdf檔案 (檔案名稱: 學號.pdf, 內容包含正確密鑰、解出明文、截圖需含moodle姓名、解出畫面)
  - 2. 三週內繳交
  - 3. 一人一組