Q_1：上網找一則關於 DDoS 攻擊的事件，並簡短分析事件中 DDoS 的攻擊模式(100 字以內)。

A_1：

事件：「臺灣史上第一次券商集體遭 DDoS 攻擊勒索事件」(相關內容在下方「參考資料」處)

攻擊模式：DDoS 攻擊是伺服器同時收到來自許多電腦組成的殭屍網路之超多的垃圾請求，使伺服器超載，無法處理合法請求，影響用戶。在此事件中，駭客透過購買 DDoS 攻擊的服務(Booter Service)可在短時間內發動洪水式攻擊，癱瘓大公司的伺服器，並趁機恐嚇、勒索金錢。

Q_2：根據 RSA 加密演算法(如下圖)，用以下給定的數字求出公鑰(N,e)和私鑰(N,d)，請寫下計算過程：

p = 11 , q = 3 , e=7

公鑰與私鑰的產生 ［編輯］

假設Alice想要通過一個不可靠的媒體接收Bob的一條私人訊息。她可以用以下的方式來產生一個**公鑰**和一個**私鑰**：

1. 隨意選擇兩個大的質數p和q，p不等於q，計算$N = pq$。
2. 根據歐拉函數，求得$r = \varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$
3. 選擇一個小於r的整數e，使e與r互質。並求得e關於r的模反元素，命名為d（求d令$ed \equiv 1 \pmod{r}$）。（模反元素存在，若且唯若e與r互質）
4. 將p和q的記錄銷毀。

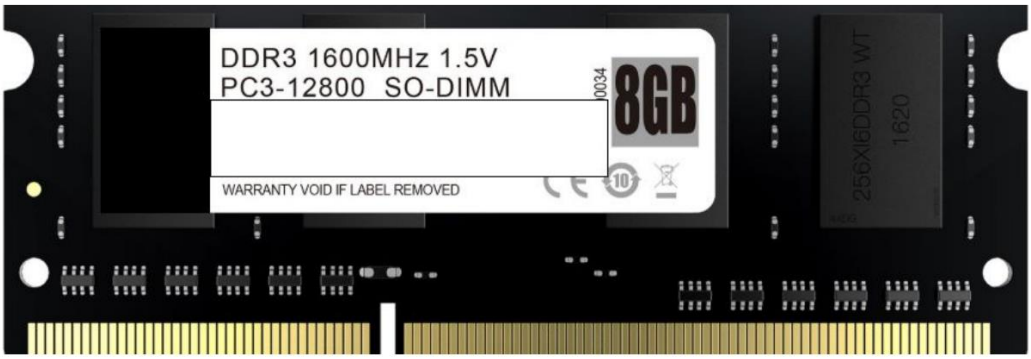
(N, e)是公鑰，(N, d)是私鑰。Alice將她的公鑰(N, e)傳給Bob，而將她的私鑰(N, d)藏起來。

A_2：計算過程如下：

1. 選擇兩個大的質數 p=11 和 q=3，計算 N=p×q=11×3=33。
2. 根據歐拉函數，求得 r=$\varphi(N) = \varphi(p) \times \varphi(q) = (p-1)(q-1) = (11-1)(3-1) = 10 \times 2 = 20$。
3. 選擇一個小於 r 的整數 e，使 e 與 r 互質，在此選擇 e=7，並求得 e 關於 r 的模反元素，命名為 d(即令 ed≡1 (mod r)並求出 d 值)，在此取 d 值為 3。
4. 故可求出公鑰(N,e)=(33,7)和私鑰(N,d)=(33,3)。

Q_3：下圖是某型號記憶體的部分示意圖,請問此類型的記憶體擁有幾個針腳(Pins)？

(提示:請根據 DDR 和 DIMM 類型,到維基百科查詢答案。不要直接用數的~助教也沒數過,不知道用數的答案對不對喔)



A_3：

Comparison of DDR SDRAM generations

Name		Release year	Chip			Bus			Voltage (V)	Pins		
Gen	Standard		Clock rate (MHz)	Cycle time (ns)	Pre-fetch	Clock rate (MHz)	Transfer rate (MT/s)	Bandwidth (MB/s)		DIMM	SO-DIMM	Micro-DIMM
DDR	DDR-200	2000	100	10	2n	100	200	1600	2.5	184	200	172
	DDR-266		133	7.5		133	266	2133				
	DDR-333		166⅔	6		166⅔	333	2666⅔				
	DDR-400		200	5		200	400	3200	2.6			
DDR2	DDR2-400	2003	100	10	4n	200	400	3200	1.8	240	200	214
	DDR2-533		133⅓	7.5		266⅔	533⅓	4266⅔				
	DDR2-667		166⅔	6		333⅓	666⅔	5333⅓				
	DDR2-800		200	5		400	800	6400				
	DDR2-1066		266⅔	3.75		533⅓	1066⅔	8533⅓				
DDR3	DDR3-800	2007	100	10	8n	400	800	6400	1.5/1.35	240	204	214
	DDR3-1066		133⅓	7.5		533⅓	1066⅔	8533⅓				
	DDR3-1333		166⅔	6		666⅔	1333⅓	10666⅔				
	DDR3-1600		200	5		800	1600	12800				
	DDR3-1866		233⅓	4.29		933⅓	1866⅔	14933⅓				
	DDR3-2133		266⅔	3.75		1066⅔	2133⅓	17066⅔				
DDR4	DDR4-1600	2014	200	5	8n	800	1600	12800	1.2/1.05	288	260	
	DDR4-1866		233⅓	4.29		933⅓	1866⅔	14933⅓				
	DDR4-2133		266⅔	3.75		1066⅔	2133⅓	17066⅔				
	DDR4-2400		300	3⅓		1200	2400	19200				
	DDR4-2666		333⅓	3		1333⅓	2666⅔	21333⅓				
	DDR4-2933		366⅔	2.73		1466⅔	2933⅓	23466⅔				
	DDR4-3200		400	2.5		1600	3200	25600				

由上圖可知：此類型的記憶體擁有 **204** 個針腳(Pins)。

Q_4：簡單說明數位訊號(Digital signal)和類比訊號(Analog signal)分別是什麼(各 100 字以內)？

A_4：**數位訊號(Digital signal)**：為離散(非連續)的訊號，由兩種訊號(0—off 與 1—on)構成，由類比訊號取樣而來，取樣數越多，越能還原真實情況，但無法 100%還原

類比訊號(Analog signal)：為連續的訊號，有強度、頻率高低(波形)之分，能表現出真實的情形，但較難儲存。

參考資料：

(1) 臺灣史上第一次券商集體遭 DDoS 攻擊勒索事件・網址：
https://www.ithome.com.tw/news/111875

(2) Telegram 遭到 DDoS 攻擊・網址：
https://www.ithome.com.tw/news/131251