1. **手工設定IP欄位的各個欄位的用途?**

IP位址(ip address): 需輸入所被分配到的Ip

子網路遮罩(subnet mask): 用來區分溝通對象是相同或不同的子網路

預設閘道(default gateway): 區域網路對外走的通道

Dns server: 當要上網時IP 要找domain name(DNS反解) 或是 domain name 要找ip (DNS正解)都是詢問所設定的這部機器。

1. 路由器(ROUTER)的功能是甚麼?

路由器是一個交通樞紐，他有許多輸入/出的PORT，從某一個PORT收一個封包近來，收進去後，他會拆解IP標頭，找出目的地IP位址，並對照路由表，決定要從哪一 個PORT送出。

**請解釋路由器(Router)的功能，及何謂閘道路由器(gateway Router)?**

提供路由(Routing)及轉送(forwarding)兩種功能，路由為決定來源封包到目的路遊憩的路徑，透過路由演算法來計算得的路由表，看是哪個網段的在進行傳送。轉送為將來源封包移送至適當的路由器輸出端，由轉送表決定，此動作為在路由器內部進行。

由多個路由器聚集成的區域稱自治系統(AS，autonomous systems)，相同AS中的路由器會有相同的路由器，其中閘道路由器為運行所有內部AS路由器的路由協定，也負責與其他不同AS的閘道路由器溝通。

1. 路由演算法(ALGORITHM)有兩大類，分別為link state 和 distance vector， 說明這兩大類的做法，資訊交換方式的不同，及相對的優缺點?

Link state:會跟其他所有路由器報告，我與誰相連，我連線的狀況如何

優點為因為分成多個獨立的Area，所以可以減少Routing Table中的資料筆數，並且用最快速度達到網路收斂。

缺點: Link-State路由演算法要維護的資料比較多，也比較複雜，一旦網路環境複雜，占用硬體設備多。

Distance vector 只跟直接相連的鄰居交換資訊

優點: 容易 維護

資源消耗低

缺點: 收斂較慢

規模大的網路頻寬會消耗較高

會產生迴圈

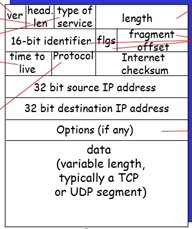
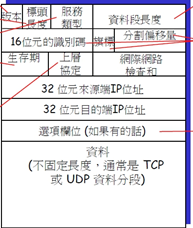
擴充性受限制

**由演算法(Routing algorithms)請列出所有的，說明操作方式與優缺點。**

連線狀態演算法(link state algorithms，LS)及距離向量演算法(distance vector algorithms，DV)，連線狀態演算法為讓每個路由器都知道所有節點的連結成本，讓路由器可以決定最佳的路徑。距離向量演算法為知道連接的鄰居和其連接的鄰居的連結成本，透過反覆計算，知道目的的位置。

訊息複雜度(Message complexity)為DV較簡單因為只跟鄰居交換，相對LS因為有n個節點，E條連結，O(nE)個傳送訊息。收斂速度(Speed of Convergence)為LS較佳，因DV收斂時間不固定，容易產生計算無窮的問題。強健性(Robustness)為LS較佳，因為在斷線時DV所需要的時間較久。

1. 說明下列ip標頭欄位的用途?

Ver: 紀錄ip version 是第幾版

Head len:標頭的長度

Type of service: 記載著封包所乘載著那些型態的資料比如語音、命令etc.

Length: 封包的總長，包括標頭及資料。

Time to live: 每經過一個路由器就減 1，擔心路由體系突然發生錯誤，造成迴圈，在網路中遶，無法達到目的。

Protocal: 記載著協定為tcp or udp 也可能為ICMP

Internet Checksum: 檢錯碼

Source IP address: 寄件人IP address

Destination IP address: 收件人IP address

Data: 封包

16-bit Identifier: 用來識別datagram，原本的ID會不同，但如果是被拆解的則會有相同的ID

flags: 為1 代表後面還有datagram

fragment Offset: 判斷是原來的第幾片datagram

1. ICMP的功能?

IP層的輔助協定，以IP的datagram 來乘載，讓主機、路由器、及gateway之間，彼此溝通有關於網路層級的資訊，主要做的事情為錯誤回報及ping。

1. 說明DHCP如何運作?

客戶端會先向廣播位址傳送封包，尋找網域內是否有DHCP伺服器，如果有的話，DHCP伺服器則會回傳ㄧ個封包，此封包內容為可用的IP位址及其他參數，則客戶端會再度發送封包向DHCP伺服器要求此組設定，之後伺服器會回傳ㄧ個同意要求的封包。

動態主機設定協定，為區域網路分配IP的一種方法，採UDP協定工作。

分四個步驟，首先是使用這對這個網路發送DHCP發現(DHCP discover)的訊息，尋找在此網路可用的DHCP伺服器，接著伺服器接受到訊息後會對此用戶發送DHCP提供(DHCP offer)的訊息，給予該用戶一個IP租約，其中也包含一些用戶的資訊，用戶接受到IP租約後再來會在發送DHCP請求(DHCP request)的訊息，向伺服器表示已經有接收到IP的租約，最後伺服器會在發出DHCP確認(DHCP ack)，向用戶傳送租期及確認資訊等資訊，而完成TCP/IP的設置。

1. NAT 的運作

透過NAT SERVER 將虛擬IP轉換成真實的IP並送出REQUEST而NAT SERVER 也會收到Response，在NAT伺服器中也記載著哪一個虛擬IP送出的，所以NAT SERVER會將Response回給相對應的IP。

1. NAT的優缺點

優點: 讓多台電腦共用一個公有IP，舒緩了IP位址不足的問題，不容易做攻擊。

缺點: 從外面的世界看不到私網，無法架站。

1. 克服NAT 無法架站的方法:

透過PORT MAPPING 就能在私網中架站。

**請解釋NAT中的轉發端口port forwarding的用途及如何運作。**減少網際網路上實體IP的使用，讓外部可以存取內網的伺服器，可透過路由器等裝置，將外部連線至主機時，將其轉向內部網路某個主機的位置和埠口，如外界對實體IP175.65.34.3:80，會將其轉到內部的192.168.50.100:20連線，是相當方便的功能。

1. 解釋　RIP 或是 OSPF ?

為INTRA-AS的路由演算法，其中RIP為 DISTANCE VECTOR，資訊只跟直接相連的交換，而OSPF屬於LINK STATE 資訊會跟其他所有路由器做交換來告知自己的連線狀況。

1. Intra-AS 有哪兩種演算法?

RIP(routing information protocol)屬於distance vector 及 OSPF (Open Shortest Path First) 屬於 link state

1. IPV6 HEADER

pri:標示不同datagram 的priority 讓某些可以支援priority 高先送的路由器先送出priority 高的datagram.

Payload len: 表示我的data有多少

Hop limit: 類似ttl，為了防止封包在網路上變成無窮迴圈所設立的個機制。

Source address: 來源位址

Destination address: 目標位址

1. Multiple Access Protocol (多重存取協定)有哪三大類，請簡述之?

Random Access: 每個節點沒有事先協調，想用時就用，所以有可能造成collision，所以在這類演算法中有兩個重要議題，第一個為如何偵測collision的發生，還有如何從collision中復原。CSMA/CD及CSMA/CA屬於這一類型的應用。

Channel Partioning: 把頻道加以切割，將每一個子頻道給一個使用者，而切割方式有兩種，第一種為TDMA，將時間切割成一個一個的TIME SLOT，同樣編號的SLOT就給同一個使用者，優點為不會有碰撞，但可能造成浪費。另一種為FDMA與有線電視相同，也有和TDMA相同的問題。

Taking Turns: 在其他兩者之間取得平衡，運作方式有兩種，第一個為polling，有一個master node會逐一的問slave要不要送資料，如果要送，就會建立一段時間。缺點為可能造成polling overhead，而master如果不運作，整個網路就會停止運作。另一種作法為token passing，有一個特殊封包，誰拿到這個封包，就能傳送資料，缺點為可能有token overhead及token 遺失的問題。

**請解釋通道分割(Channel Partitioning)、隨機存取(Random Access)及輪流存取(Taking turns)。**

通道分割(Channel Partitioning)為將通道分割成小塊(如時槽、頻率、碼)，讓這些小塊分配為每個節點利用。

隨機存取(Random Access)為不分割通道，但允許碰撞，從碰撞「復原」。

輪流存取(Taking turns)為節點可以輪流，但是要傳送較多資料的節點可以傳送較長的時間。

**請解釋多重存取協定(Multiple Access protocols)。**決定節點如何分享通道的分散式演算法。例如，決定節點何時能夠傳送。必須使用通道本身來傳送有關通道分享的通訊，沒有不同頻帶的通道做為協調的功能。

1. 解釋CSMA/CD?

有兩部分，CSMA為在送之前，先聆聽是否有人送，如果沒有就將封包送出。

CD為一邊送封包一邊聽，如果聽到的和所送出的相同，表示沒有發生COLLISION(碰撞)但如果不同，表示發生碰撞。

**請說明乙太網路存取方式CSMA/CD(Carrier Sense Multiple Access with Collision Detection)。**

載波感測多重存取／碰撞檢測，為在傳送框訊同時進行偵測是否會發生碰撞，若發生碰撞，則在固定時間內等待隨機的時間，再次傳送，若依舊碰撞，則採用截斷二進位指數避退演算法(Binary exponential backoff)進行傳送。即十次之內停止前一次「固定時間」的兩倍時間內隨機再發送，十次後則停止前一次「固定時間」內隨機再發送。嘗試16次之後仍然失敗則放棄傳送。

1. ARP(Addressing Resolution Protocol) 的用途及運作方式?

每張網路卡都有ARP TABLE記載著 IP位址與MAC address之間的對應關係，如果要尋找的MAC ADDRESS不再ARP TABLE，則會以廣播的方式來訊問，並以單播來回傳。ARP表不需要設定，需要會自動詢問。

為透過目標裝置的IP位址，查詢目標裝置的MAC位址，以保證通訊的順利進行。每台主機都會有ARP快取表，紀錄IP對應的MAC，若今天A要傳送封包給B但B沒有在A的ARP快取表中，A會廣播ARP查詢封包，到區域網路的每個位置， 當收B收到ARP封包後會傳MAC位置給A，最後A會將B的IP-MAC對存在ARP快取表上，直到資訊逾時刪除。

1. Hub與 switch 的差別?

Hub為從一個洞口送進封包後，封包會從其他洞口送出，所以封包還是屬於同一個collision 的domain.

Switch 在每一個port都會有一個獨立的頻寬，只要通訊的對象不互相牴觸，他們能夠各自擁有switch所提供的頻寬。

差別在於集線器Hub為半雙工，而交換器switch是全雙工，而透過集線器在傳送封包時，會廣播每個主機，但只會有一台主機會是正確，而其他都會丟棄，而會分享頻寬。但交換器會記錄每個port所對應的MAC位置，能更有效率的傳送封包。

1. 解釋CSMA/CD (參考 14) 並且說明 EXPONENTIAL BACKOFF

一但發生碰撞各自延遲一段時間再重新嘗試，DELAY時間則由亂數產生，第一次碰撞從0到1之間亂數產生一個數字，每次碰撞則DOUBLE亂數範圍。

若發生碰撞，則在固定時間內等待隨機的時間，再次傳送，若依舊碰撞，則採用截斷二進位指數避退演算法(Binary exponential backoff)進行傳送。即十次之內停止前一次「固定時間」的兩倍時間內隨機再發送，十次後則停止前一次「固定時間」內隨機再發送。嘗試16次之後仍然失敗則放棄傳送。

1. PLUG AND PLAY

如果要去的目的已經在SWITCH TABLE當中，就從特定的PORT走，如果不再SWITCH TABLE當中，則以廣播形式詢問，而當有封包進去，SWITCH TABLE 就會記錄下所進來的PORT。

.

1. SWITCH VS. ROUTER

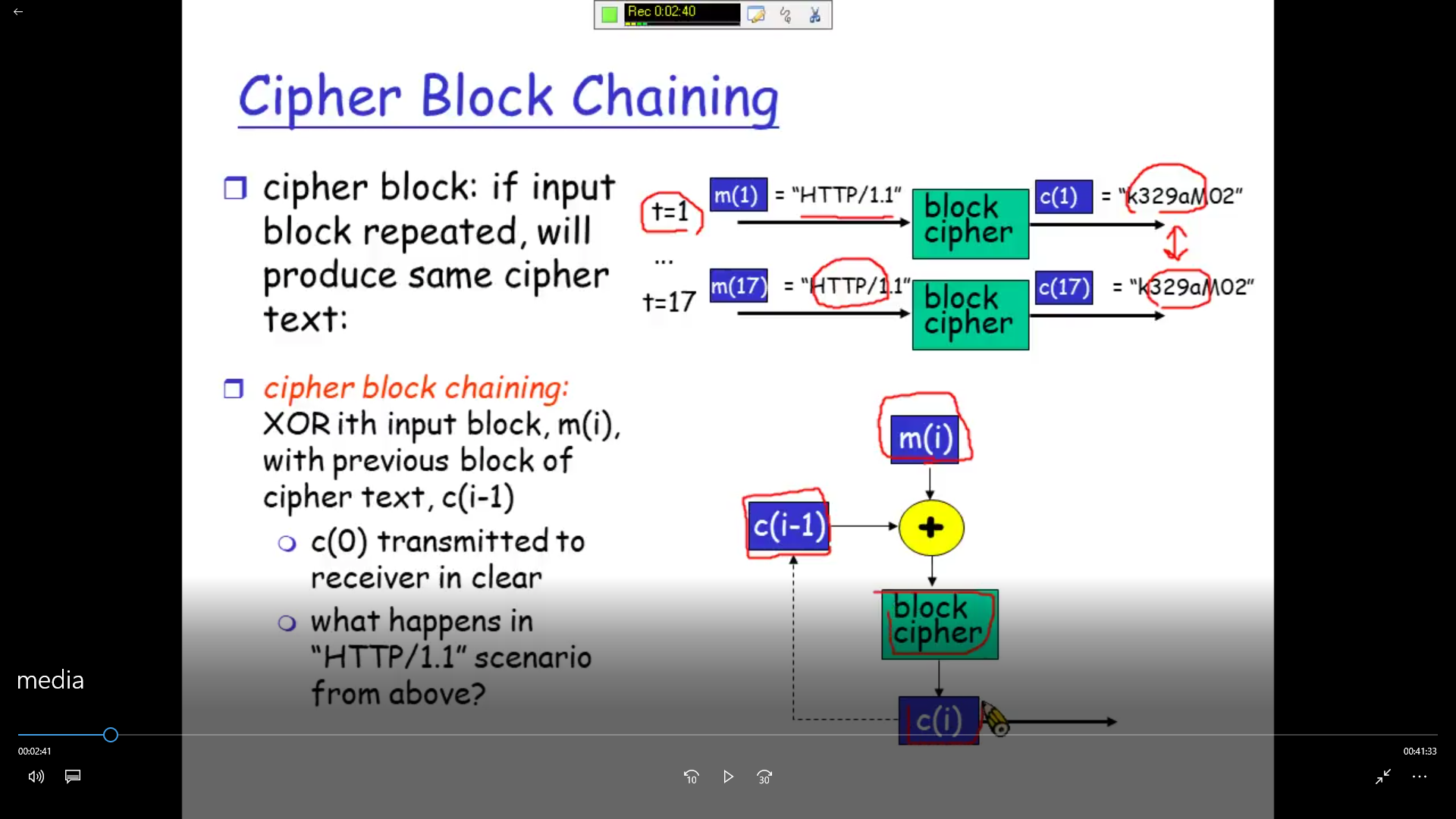
相同為都是用STORE AND FORWARD 的方式，

不同

ROUTER 是網路層的裝置並由路由表及路由演算法實現，根據收件人IP位址並對照路由表決定從哪一個PORT送出。

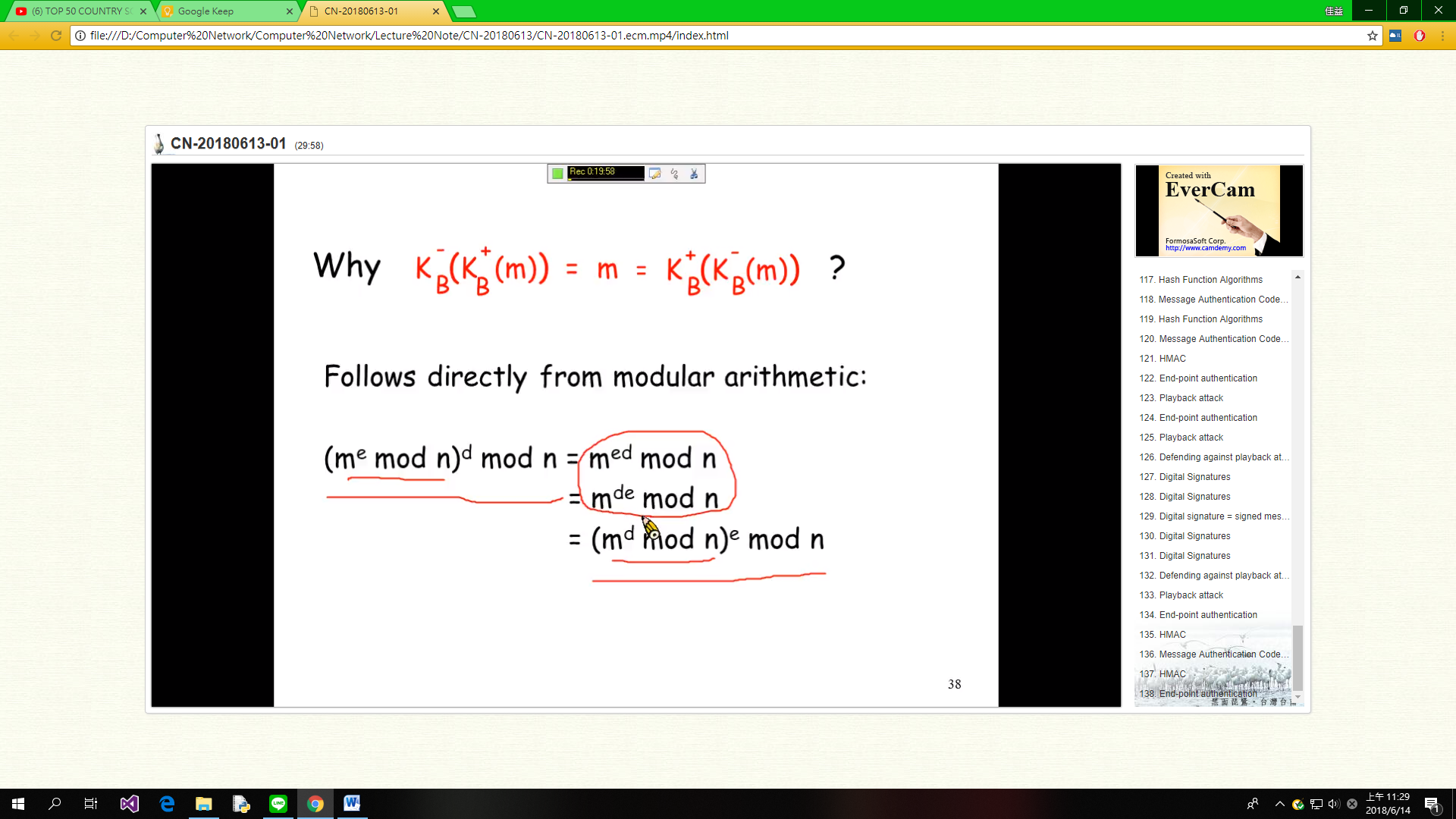
SWITCH 則為鏈結層的裝置，再FORWADING時是根據收件人網路卡卡號。SWITCH由SWITCH TABLE及學習演算法來實現。

1. 解釋名詞:
2. Confidentiality: 資料保有私密性，通常會對訊息加密後傳送，當收到訊息時再進行解密。
3. Authentication: 確認溝通的對方是真正所想溝通的人
4. Message Integrity: 在訊息的傳遞過程中，沒有被串改過
5. Access and Availability: 資訊系統能夠正常運作，並讓正常的使用者存取資訊。與此直接相關的為分散式阻斷式攻擊。
6. 壞蛋可以對網路系統所做的事?
   * + 1. 竊聽及主動的增加一些訊息到此連線中
       2. 將來源資訊偷改掉，讓對方以為是自己想溝通的人。
       3. Hijacking: 將一個正在進行的連線取代掉，讓對方以為自己所在溝通的對象是自己想溝通的對象
       4. 阻斷式攻擊，透過耗費受害主機的平寬及資源讓正常使用者無法使用。
7. Cipher Block Chaining的運作方式及目標(plus 圖)?



將明文裡第i個block與密文第i-1個block進行xor加到block cipher 產生出第i個block的密文。C(0)則是以亂數產生。目標讓相同明文的block，能夠產生不同密文的block。

1. RSA 證明



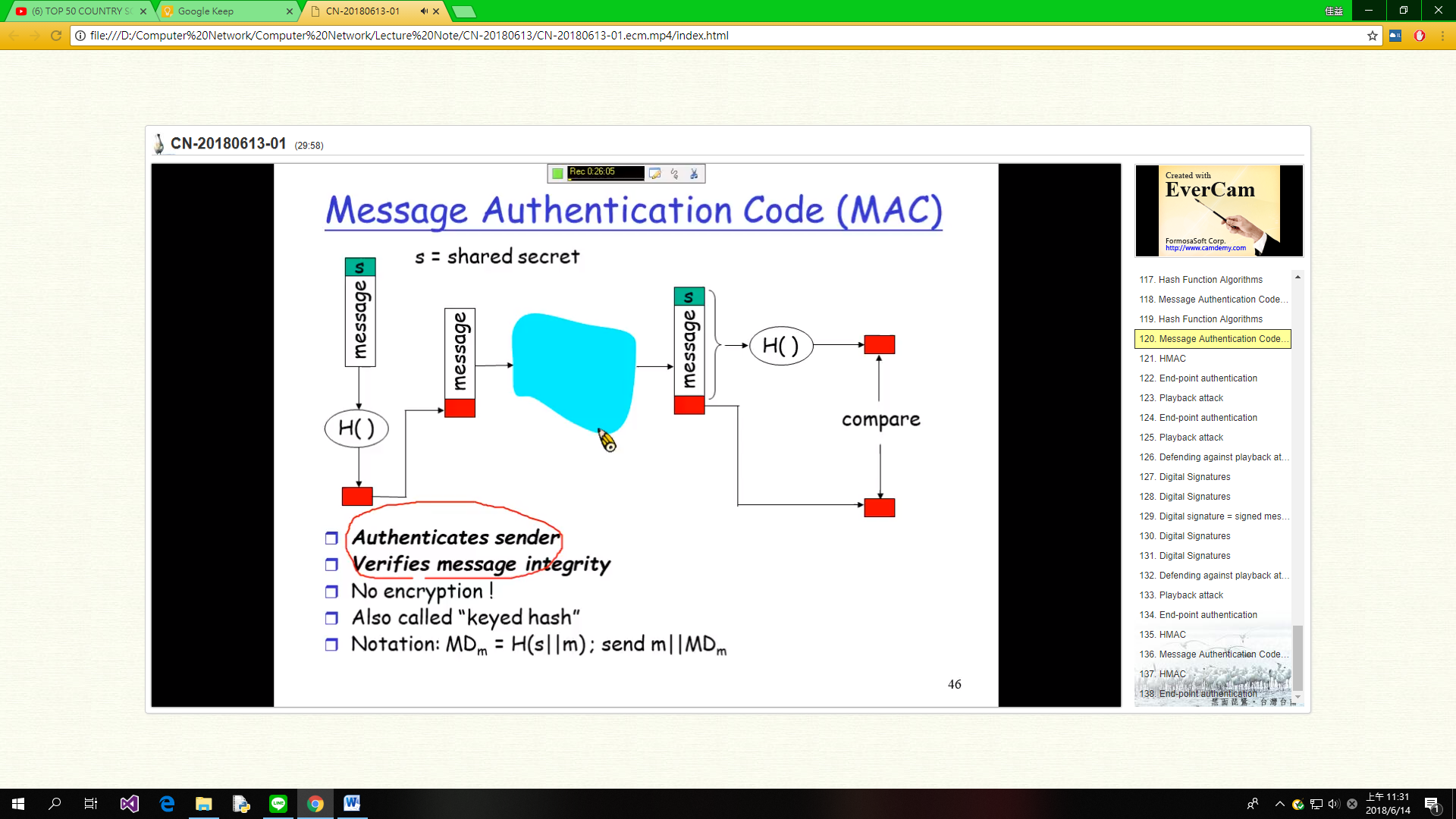
m為欲加密訊息

n為在製作公私鑰的過程中 以兩個大質數(p and q)相乘的數值

而e和d 則是先求出z=(p-1)\*(q-1)，再求ㄧ個小於n(wiki紀載為小於z)並與z互質的e，之後求出ㄧ個d可以使e\*d除於z的餘數為1

則n和e為公鑰 n和d為私鑰

1. 如何做message authentication code**(MAC)**?

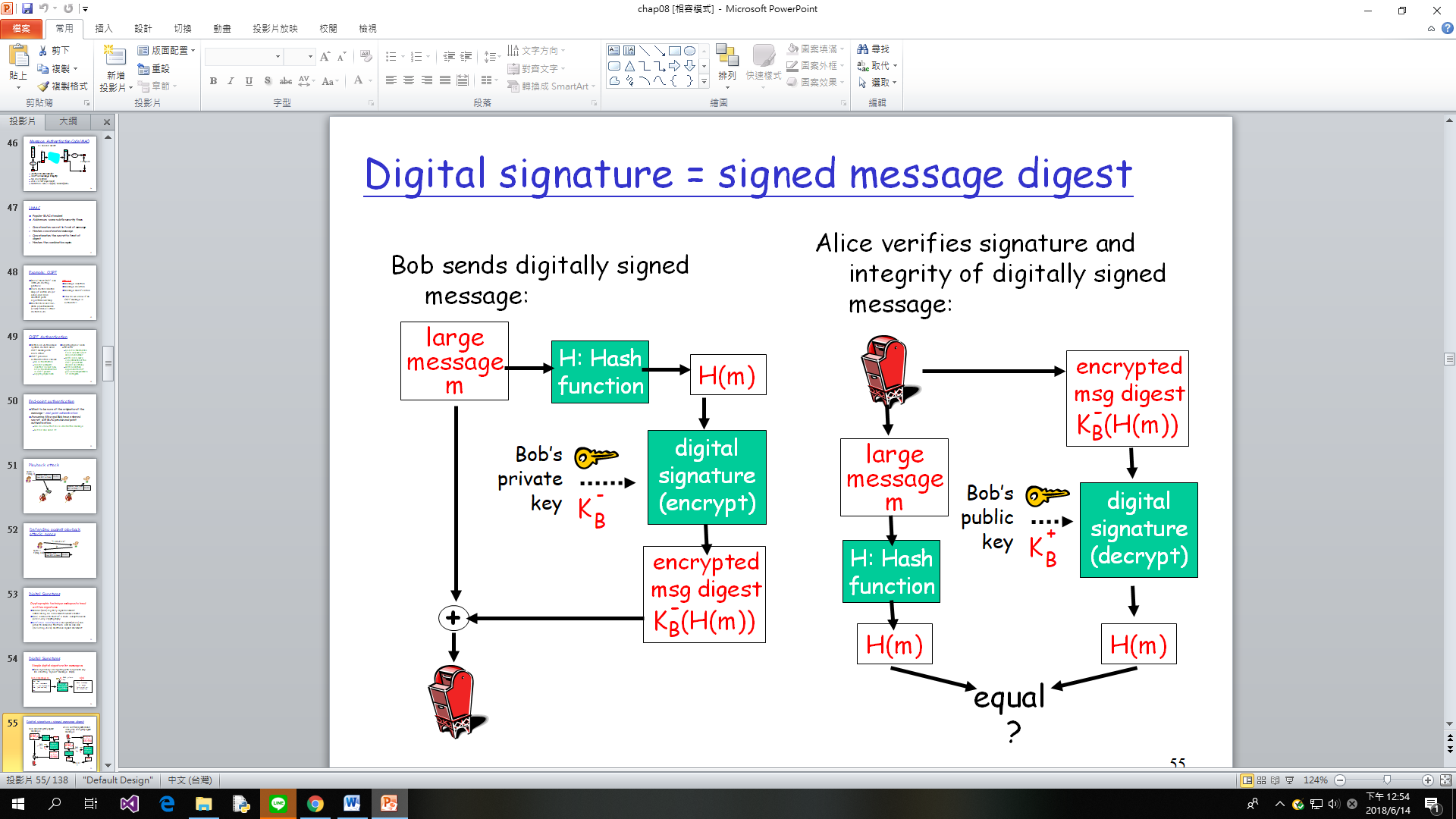


在訊息前加上傳送者與接收者彼此知道的祕密訊息，將秘密訊息與要送的訊息，串起來經過hash function產生digest，將message 與digest送出，送出後，再將訊息接收端也知道的訊息經過hash function產生digest再進行比對。做到authentication及維護資料不被串改。

1. 如何避免重播?

避免訊息被重播，每次都加上一個及時及只用一次的訊息，所以產生的mac是由message，secrete，及nonce所產生，藉由這機制就可以避免被重播。

1. 數位簽章



將傳送者的文件，透過hash function找出digest，然後只對digest簽章，而接收者到後會將digest解碼及將訊息透過同樣的hash function找出digest，在比較簽章所解出的digest與透過同樣hash function所解出的是否相同，如果相同表示文件未被串改及確認文件來自於原本的傳送者。

1. 對稱金鑰及公鑰的不同?

對稱金鑰為在收送雙方需要有共同的鑰匙。

公鑰系統: 每個個體有兩把鑰匙，公鑰及私鑰，公鑰是讓別人知道的，私鑰只又自己知道。

1. DES 的運作方式?

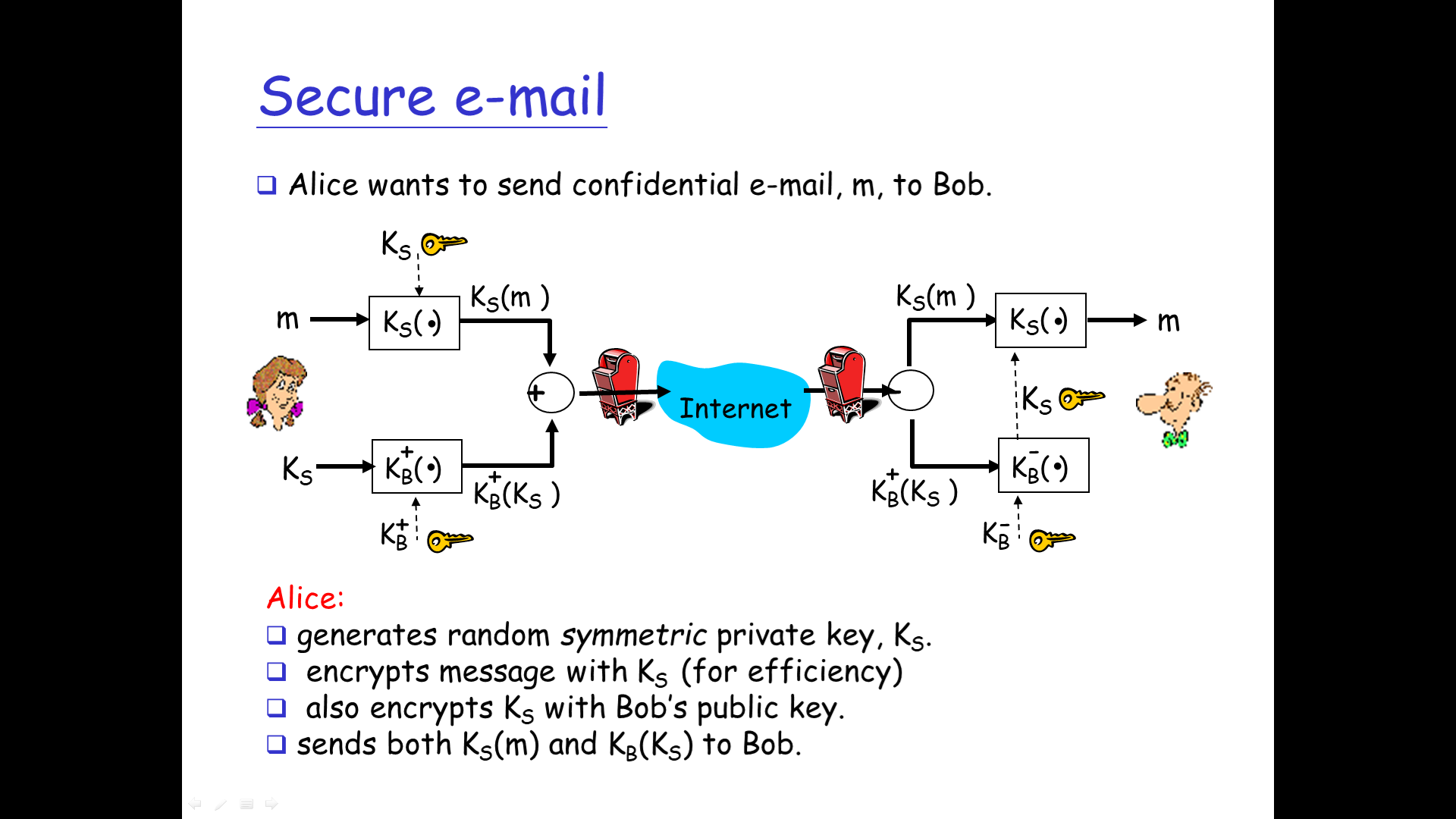
透過一連串的 substitution 及 permutation 將資料打亂。

1. 如何用公鑰系統達到 confidentiality 及 authentication?

Confidentiality: A要傳訊息給B先用B的公鑰來加密，B再用自己私鑰解密。

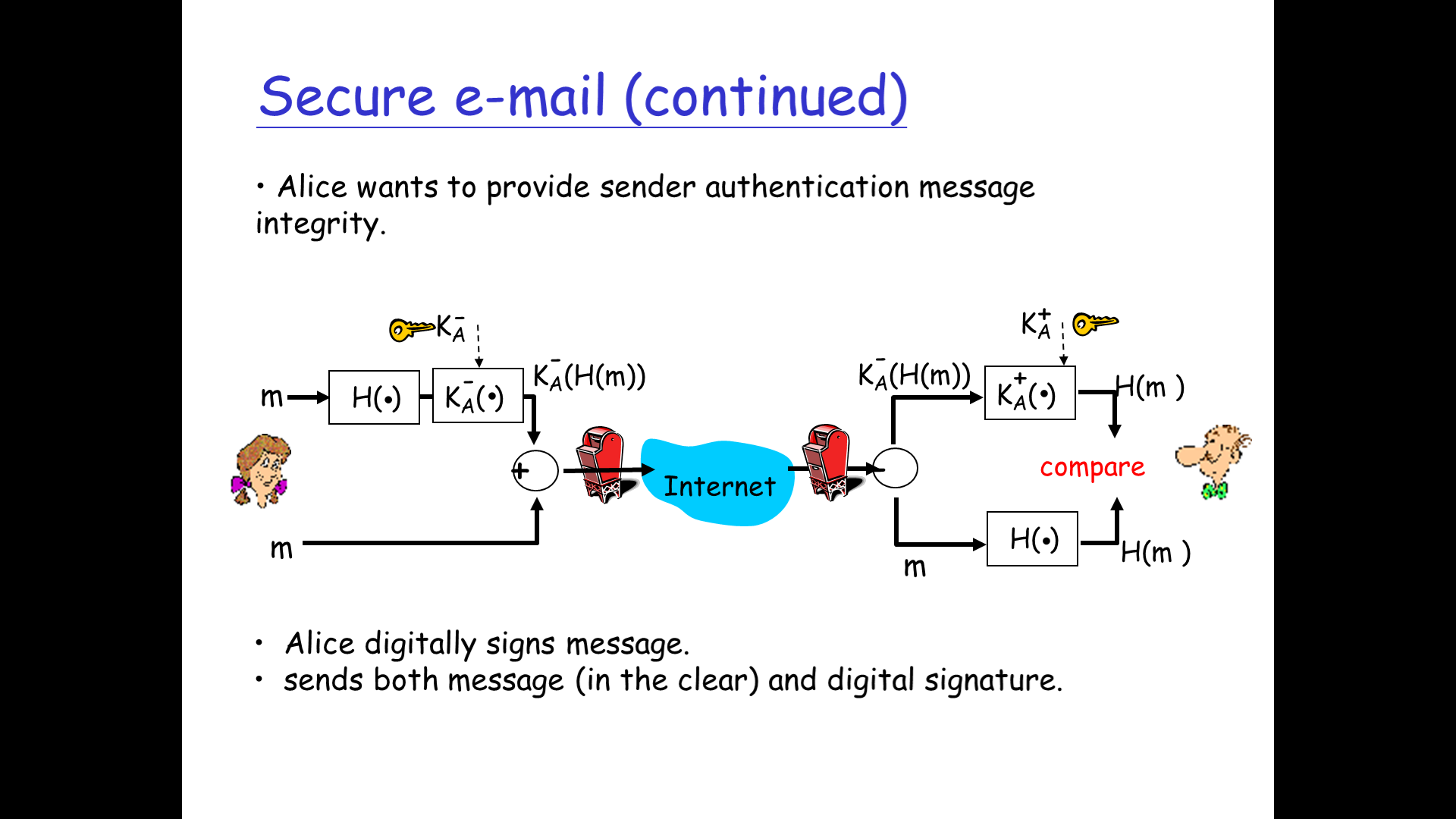
Authentication: B要傳訊息給A，B用自己的私鑰加密，A在用B的公鑰解密。

1. 看圖說故事，解釋為何可以達到Confidentiality?



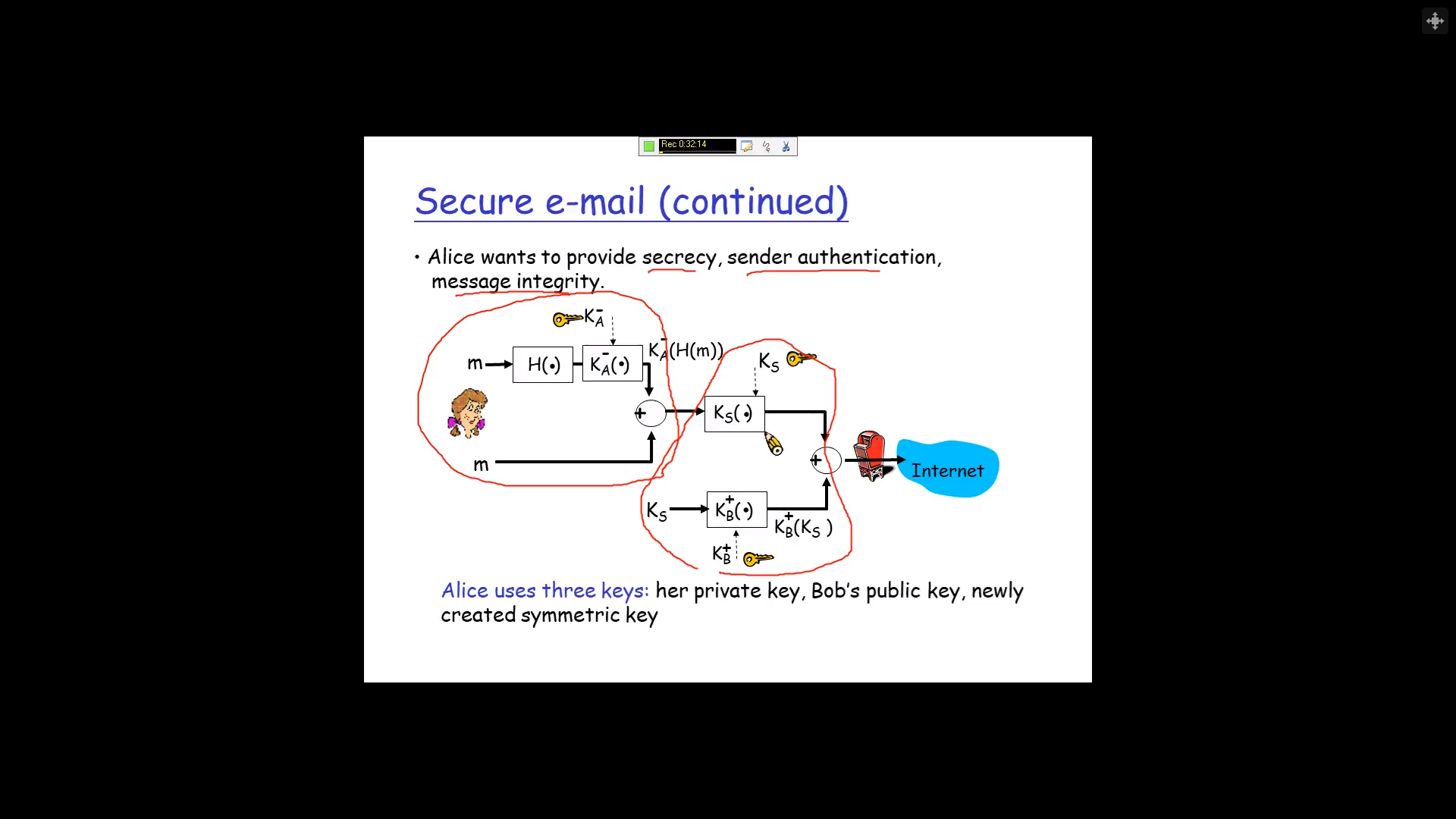
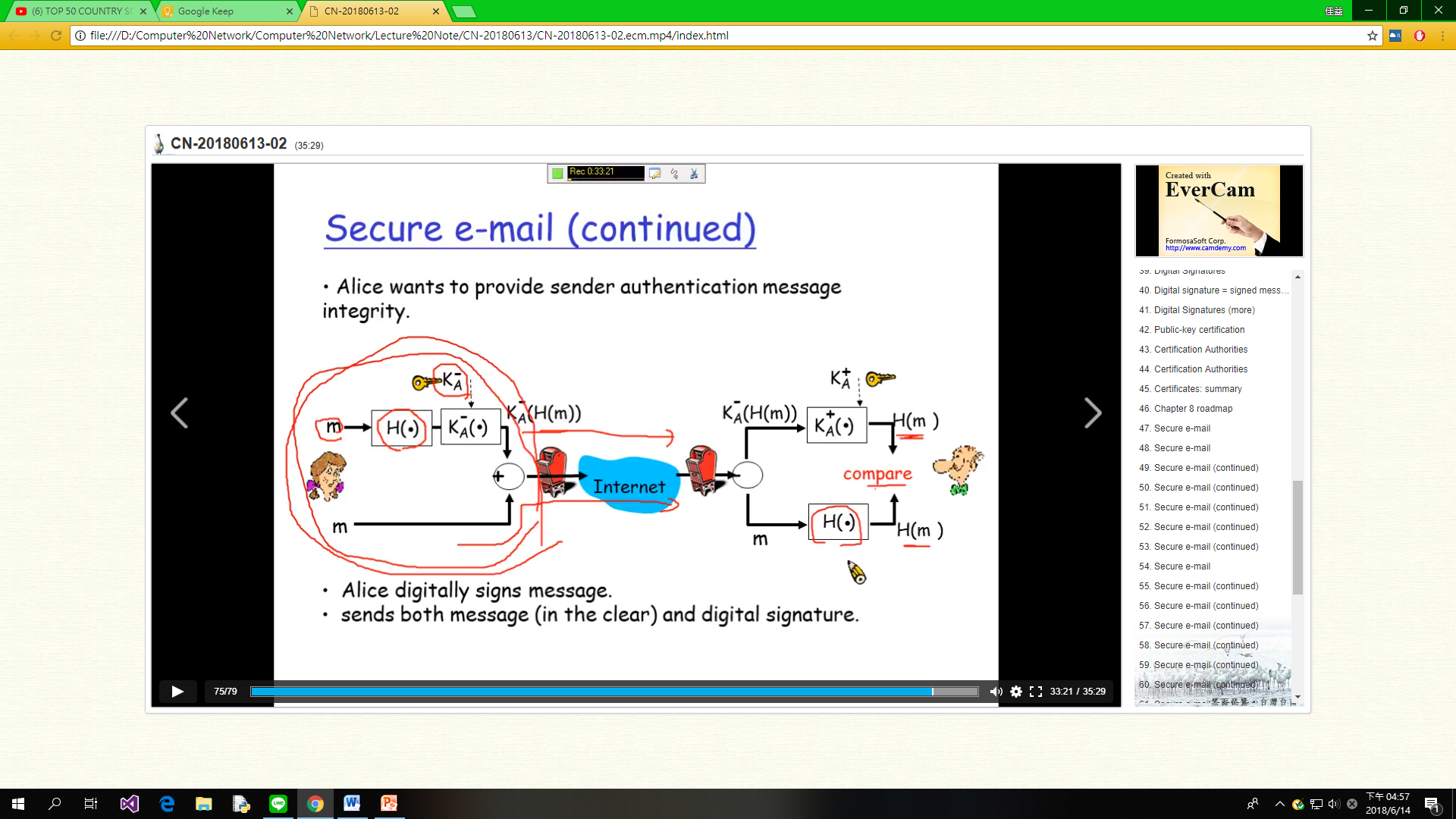
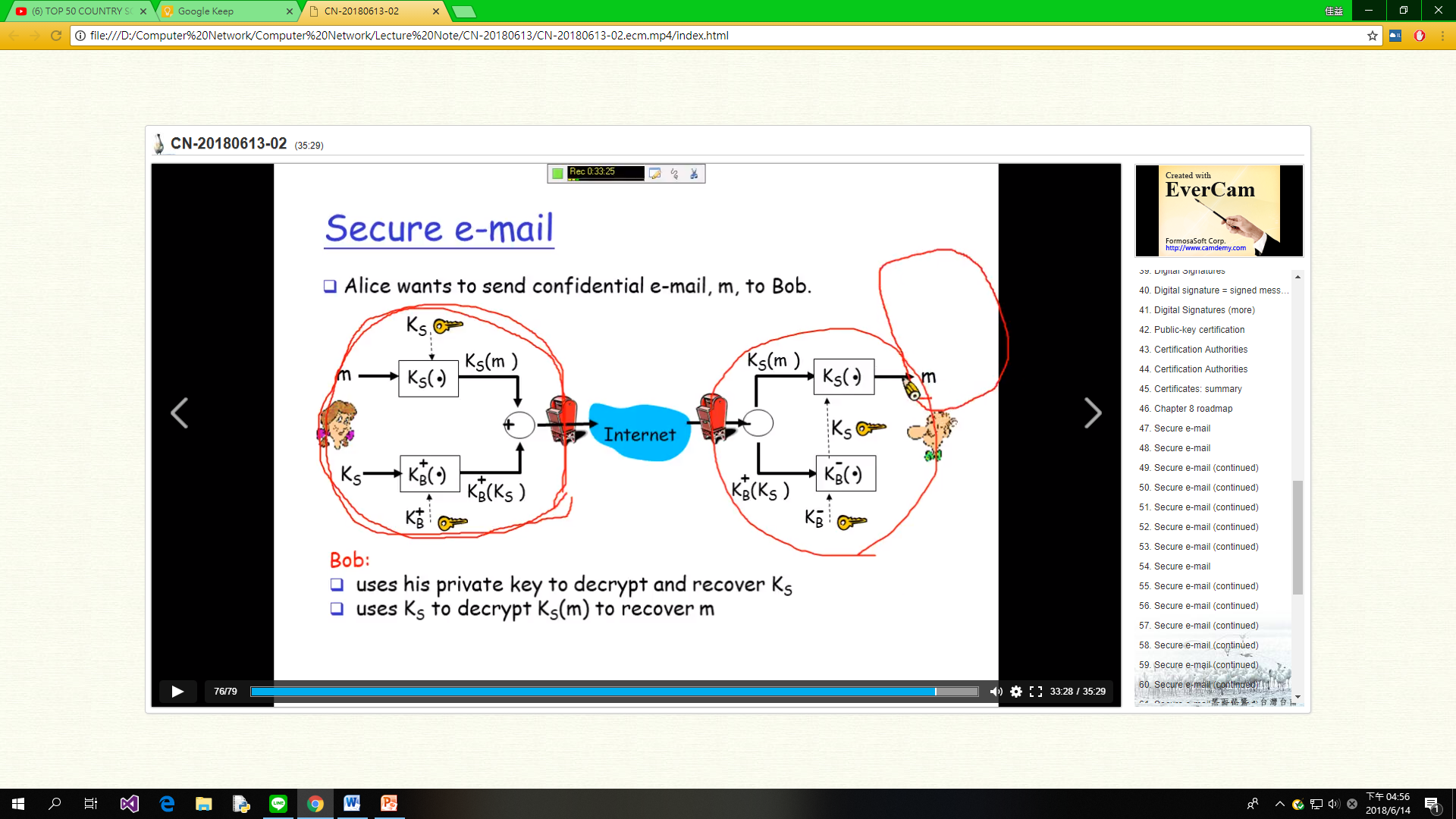
把訊息加密，如使用AES或DES產生加密後的密文，而金鑰用接收者的Public Key 來加密，然後將兩份文件送出，接收者收到後會用自己的私鑰將鑰匙取回來，並將密文解回明文。

1. 追求authentication?



將信件內容，經過hash function，用傳送者自己的私鑰加密，然後與m同時送出，收到後m用同樣的hash function 得到訊息digest，接收者再用傳送者的公鑰將原本的digest取出，然後做比對，如果相同代表訊息沒被更改過，且為所想的那個接收者所送。

1. 如何追求confidentiality 及authentication 及integrity?



首先將欲發送的資料m利用雜湊函式取得digest之後利用發送者的私鑰加密，

將資料m與加過密的digest一起使用對稱金鑰Ks來加密之後，再用接收者的公鑰將Ks加密並與剛加過密的資料傳送出去。

而接收端接收到資料後，利用自己的私鑰解出Ks之後，利用Ks把加過密的資料還原，之後將資料m經過相同的雜湊函式取得digest並將原本加過密的digest使用發送者的公鑰去解密後開始對照是否與自己算出來的digest一樣，如果一樣則代ㄒ表訊息沒被竄改過。

1. Firewall 的功能?

介於內網與外網之間的軟硬體設備，可以過濾封包，也可以保護外面的人不會進到內網，及限制內部的人存取外部資料。

1. 解釋下列各部分如何構成是甚麼?

New IP header: 寫著VPN Server 的ip address

Original IP header: 寫著從總公司電腦到哪一部電腦

ESPheader 為讓接收者知道如何處理。

SPI: 讓接收者知道我是根據哪一個SA來加密。

Seq: 防止replay的攻擊。

Padding:補到整數個block

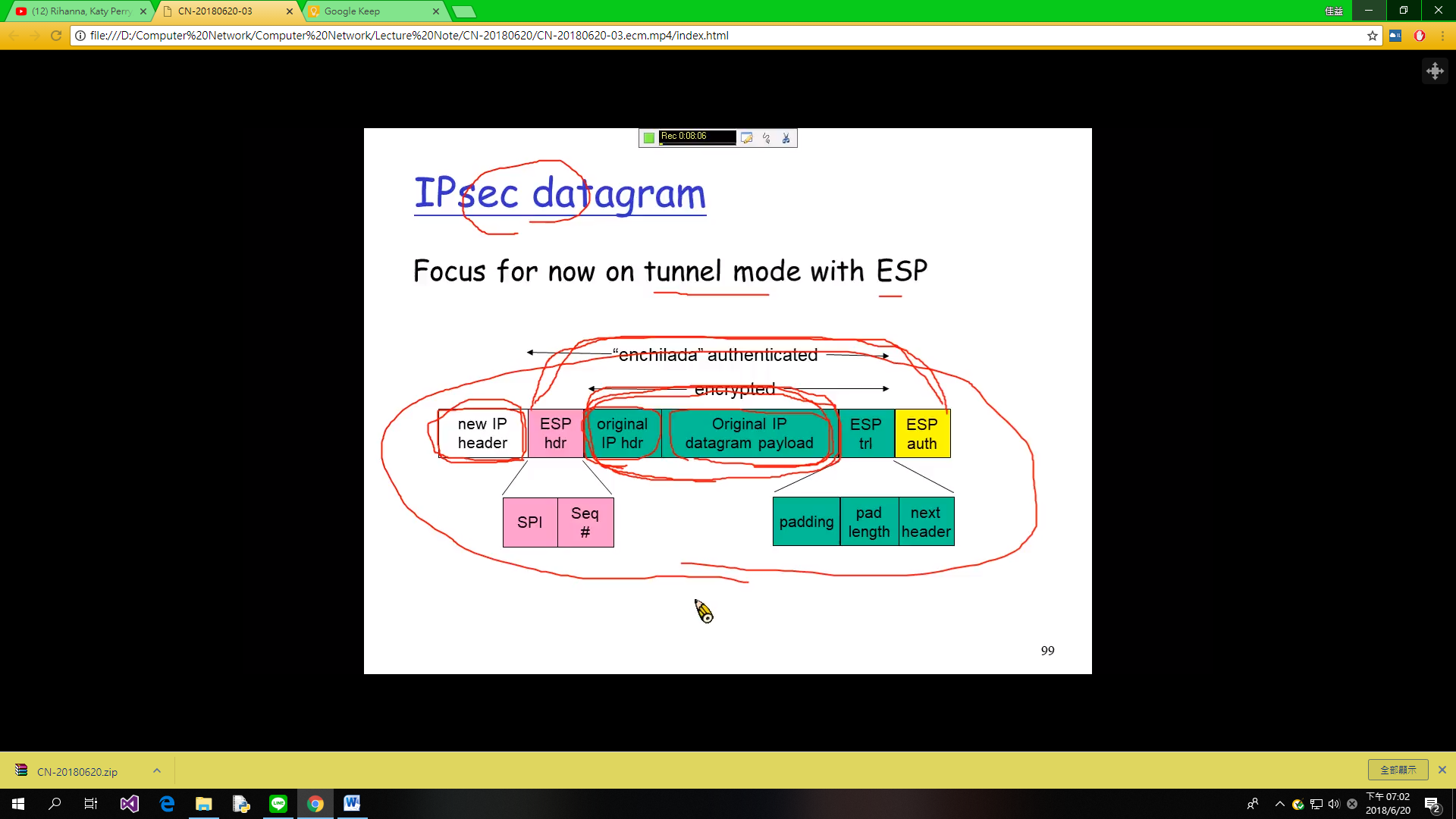
Padding length: 補了多少個BLOCK

Next header: 告訴我們封包的格式如tcp

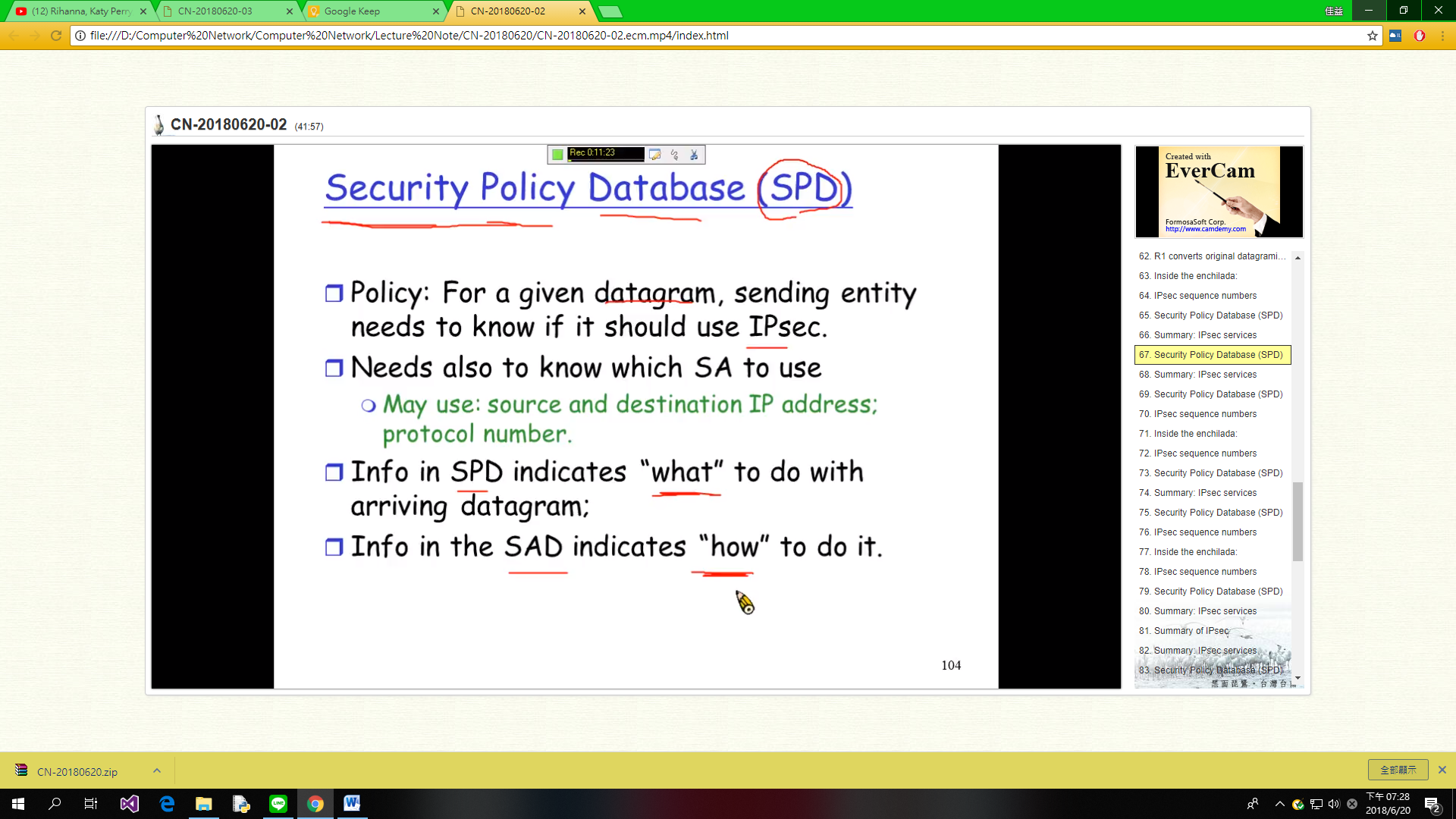
ESP auth: 透過 hash function 所產生的。

1. 如何把一個正常datagram轉換成 IPSEC 的datagram?

在原本的datagram當中加上一個ESP trailer，然後將原本的封包及ESP trailer用SA裡所指定的 algorithm 或key 來加密，加密後在前面補上ESP的HEADER，然後對ENCHILADA 透過HASH FUNCTION產生ESP AUTH，加到ENCHILADA後將新的IP header放到最前面。



1. SPD與 SA?



SPD為告訴我們是否需要將資料轉成IPSEC。

SA為告訴我們要如何將資料轉成IPSEC

37.CA憑證

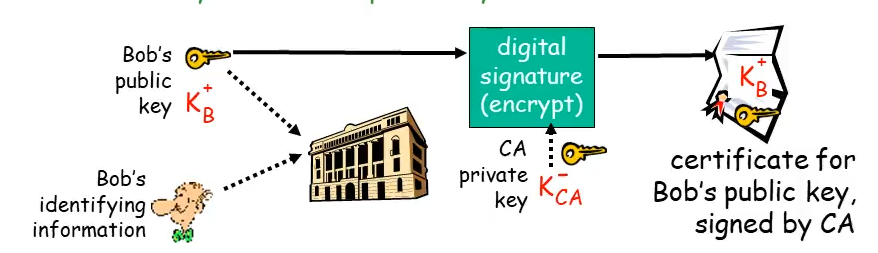
CA伺服器會有ㄧ個資料庫，當想要某個人的公鑰時可以向CA伺服器詢問，CA將會提供有公信力的答案。

當一個個體E想要申請憑證時:

step1:E會向CA機構證明自己的身分。

step2:CA伺服器將E與其公鑰建立起關係製造憑證。

step3:之後CA伺服器將會簽署此憑證，憑證上會記載E和其公鑰的資訊。



38.Intrusion Detection Systems:

檢查封包關聯性，或檢查病毒特徵碼，察覺到異常的行為並且自己或透過防火牆來攔截。

-----------------------------------------------------------------------------------------------------------

**1. 請解釋連階層的錯誤偵測(Error Detection)及錯誤更正(Error correction)。**

錯誤偵測為因訊號衰減或雜訊所產生的錯誤，接收端偵測到錯誤的存在，通知傳送端重新傳送訊息或是將訊框丟掉。

錯誤更正為不憑藉重新傳送，接收端辨識並更正位元錯誤

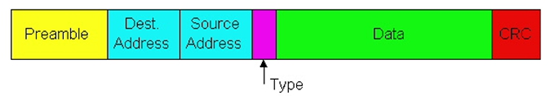
**2. 請解釋連階層的服務之一，流量控制(Flow control)。**

調整相鄰傳送端和接收端節點之間的步調。

**3. 請解釋半雙工(half-duplex)。**

指在連結兩端的節點可以雙向傳送，但無法同時。

4. **請解釋下列Ethernet的欄位(Ethernet Frame Structure)用途。**

****

**Preamble:**前置位元，由8位元組組成，第一位元組為10101011，後7位元組都為10101010，用來同步傳送端和接收端的時脈速率。

**Dest. Address:**目標位址，有6位元組，指的是MAC的位址。

**Source Address:**來源位址，有6位元組，指的是MAC的位址。

**Type:**類型，表示上一層所使用的協定。

**Data:**資料欄，資料欄包含真正要傳送的訊框資料，由於偵測碰撞信號的需要，傳送訊框長度至少需64 Bytes，扣除表頭(Header)及FCS剩下46 Bytes，此46 Bytes是最小需求。

**CRC:**循環冗餘校驗，有4位元組，接收端會檢查此一欄位，如果錯誤就會丟棄此一訊框。