1. ASCII → 二進制

p	l	a	i	n	t	e	x	t
0x70	0x6C	0x61	0x69	0x6E	0x74	0x65	0x78	0x74
01110000	01101100	01100001	01101001	01101110	01110100	01100101	01111000	01110100

2. 將前面的9組二進制的8bits串接。

011100000110110001100001011010010110111001110100011001010111100001110100

9x8=72 bits ※

3. 把上面的72bits切成6bits一組⇒011100, 000110, 110000, 100001, 011010, 010110, 111001, 110100, 011001, 010111, 100001, 110100 共12組。

4. 將前面12組 → Radix 索引 → 字元

(10進制)	28	6	49	33	26	22	57	52	25	23	33	52
	c	G	x	h	a	W	5	0	Z	X	h	0

Final answer: cGxhaW50ZXh0 ※

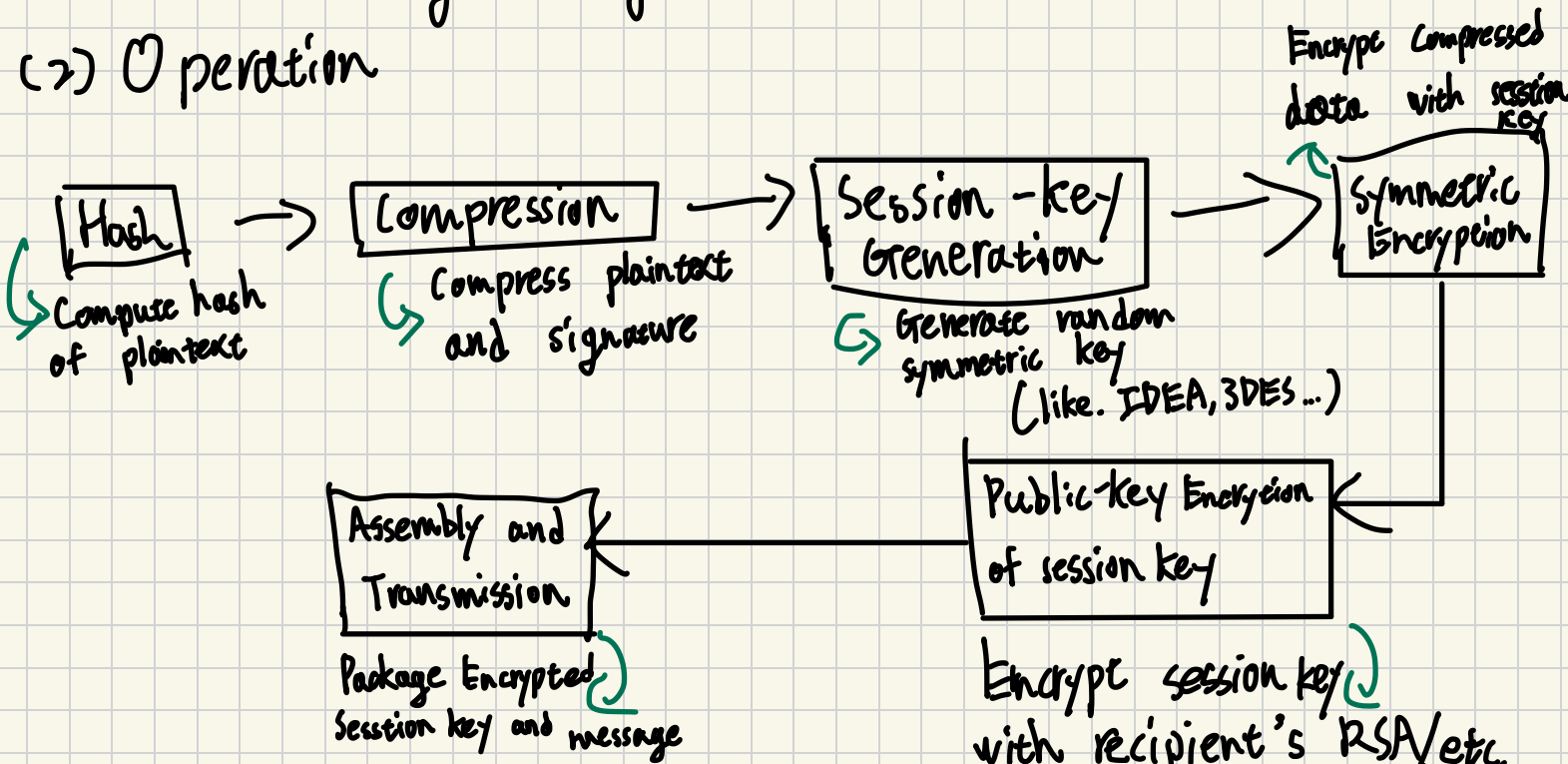
2. About the PGP

PGP = Pretty Good Privacy.

(1) Definition

- Is a software application developed by Phil Zimmermann in 1991 to encrypt and decrypt emails and files, providing both confidentially and authentication.
- Is a digital signature.

(2) Operation



(3) Problem & Solution.

Symmetric encryption is efficent but requires a shared secret key. Distributing this key over insecure channels risks exposure. This is known as the key distribution problem.

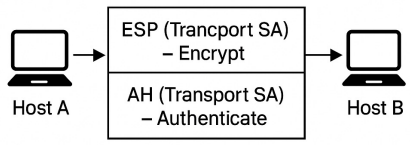
(3-1) PGP (Public-key Solution)

PGP addresses this by employing asymmetric (public-key) encryption solely for the session key. The Workflow is

Sender generates a random session key → Sender encrypes the session key with recipient's public key. → Encryted Session Key is prepended to the symetrically encrypted message

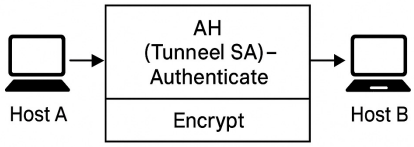
Recipient uses their private key to recover the session key and decryt the message.

3.



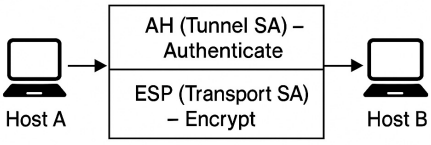
→ Transpore Adjacency

(Encryption before Authantication)



→ Transpore SA inside Tunnel SA

(Encryption before Authentication.)



→ Transpore SA inside Tunnel SA

Authentication before Encryption.)

4.
Cardholder : consumer who hold a payment
Merchant : the seller of goods who accept SET payment
Issuer : the cardholder's bank that issue the payment card and authorize payment
Acquirer : the merchant's bank that processes the transaction and forwards payment request to the issuer
Payment Gateway : The secure server that routes payment messages among the merchant, acquirer, and issuer.
CA : the trusted third party that issue digital certificates to authenticate cardholders and merchants

dual signature is cryptographic mechanism in SET that links Order information (OI) and Payment Instruction (PI) - without revealing one to the wrong party - The cardholder computer separate hashes of OI and PI, concatenates these hashes, and then signs the result with their private key.

Purpose : integrity : ensure neither the merchant nor issuer can alter the data without detection
confidentiality : the merchant see only OI, not PI, issuer see only PI, not OI
Binding : Proves that OI and PI belong to same transaction

5. Transport mode : encrypts only payload of an IP packet; the original IP header remain intact. commonly used for end-to-end security between hosts

Tunnel Mode : encrypts the entire original IP packet and then encapsulates it within new IP packet a fresh header

6. HTTPS是將HTTP封裝於TLS (or SSL)，提供加密、資料完整性檢查與伺服器身份驗證

加密：HTTP header : cookie、授權標記
HTTP body : 表單資料、JSON等
URL路徑

未加密
IP/TCP標頭

黃敬泓 黃韋傑 張世鵬