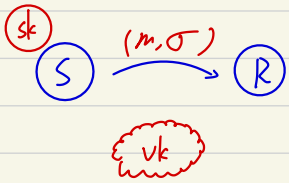
驗證

Signature { Authentication : 驗證性
Integrity : 完整性
Non-repudiation : 不可否認性

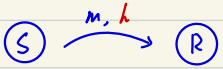
msg : m
signature : σ



Syntax of Digital Signature

- Gen (λ) → sk, vk → verification key (public)　(by S; sk: signing key)
- Sign (sk, m) → σ
- Vrfy (vk, m, σ) → accept / reject

Quiz:

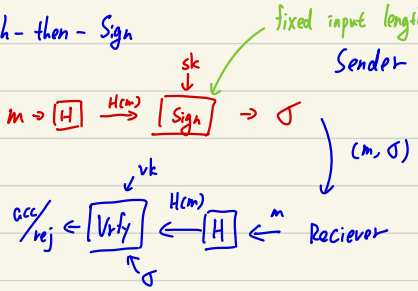


h = H(m)
Hash function

verify H(m) =? h，這樣是否有 { Authentication / Integrity / Non-repudiation }

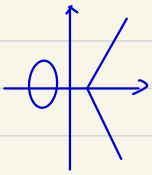
1. Authentication (Is msg from S)　X
2. Integrity (Is msg not modified)　O
3. Non-repudiation (Is h by S)　X

Hash-then-Sign



$y^2 = x^3 + ax + b \mod p$ (p: prime) → 因為電腦無法計算無限大

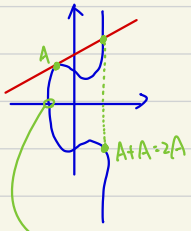
$x, y, a, b \in Z_p = \{0, \cdots, p-1\}$



Tradition: $a + b = c$

EC : $A + B = C$

$A + \infty = A$



if $y=0$, no spot 叫 B，稱之為"無限原點"

P: a point in $\mathbb{E}$ ← group define by a EC (橢圓曲線)

If p is a generator, $\mathbb{E} = \{P, 2P, \cdots, (p-1)P\}$

$P + Q = R$: EC operation

$\alpha P \in \mathbb{E}, \alpha \in Z_p$

EC hardness : Given $(P, \alpha P)$, find $\alpha \in Z_p$

(EC Discrete Logarithm Problem) P is a generator of $\mathbb{E}$

(ECDLP)

什麼是 Generator

以乘法 mod 7 為例 $\{0, 1, \cdots, 6\}$

2^n : 2, 4, 1, 2, 4, 1 ⋯

3^n : 3, 2, 6, 4, 5, 1, ⋯

↑ is generator，可跑完 $\{\}$ 所有數

ECDLP : $\mathbb{E}$ is an Elliptic Curve as a group

Consider a generator P and another element T

the DL problem is to find the integer d

where $1 \le d \le \#\mathbb{E}$. s.t. $T = dP$

Elliptic Curve Digital Signature Algorithm (ECDSA)

Gen (n) : Let p be a prime, $\mathbb{E}$ is EC over mod P

P is the generator of $\mathbb{E}$

$vk = (\mathbb{E}, P, \alpha P)$

$sk = \alpha \in \mathbb{Z}_p$

Sign (sk, m) : 1. random $r \in \mathbb{Z}_p$

2. Compute $\sigma_1 = rP \in \mathbb{E}$

3. Compute $\sigma_2 = r^{-1}(H(m) + \alpha \cdot u) \in \mathbb{Z}_p$, $u = H(\sigma_1, vk, m)$

$H : \{0,1\}^A \to \mathbb{Z}_p$

Vrfy (vk, m, σ)

$\sigma_2 \cdot \sigma_1 = ?$

$(H(m) + \alpha u)P = H(m)P + u(\alpha P)$

if $\sigma_2 \cdot \sigma_1 == H(m)P + u(\alpha P)$: return True

else : return False