(1)

1) ~~La clau privada de Bob~~
La clau pública de l'Alícia

2) La clau pública de Carlota

(2) - És molt més ràpid signar el hash que el vídeo complet
- Si canvia qualsevol element de la película, el hash canvia completament, assegurant integritat.
- Mètode molt més ràpid i igual de segur (si es xifra i es fa el hash amb els paràmetres correctes)

(3) - Validar que ha estat signat per una Autoritat de Certificació de confiança
- Comprovar que la data actual sigui després de "Not before" i "Not after" del certificat
- Comprovar que la identitat del Subjecte sigui la correcta, per exemple, amb el nom de domini com "www.uab.cat"

(4) pas 3: $h = r + b \cdot x \pmod{p-1}$ → pas 4: $c \cdot y^b = g^h \pmod{p}$

Si $b = 0$ sempre,

$h = r + b \cdot x = r$

$y^b \cdot y^0 = 1$

(pas 4) $c = g^r = g^h$ → ~~El~~ pel verificador, sempre serà cert, no pot saber si el provador coneix x o no realment

(5) Abans d'enviar el nombre proposat, cada participant ~~ha~~ ha d'enviar un hash(prefix || n), on n és el nombre escollit i el prefix s'escull immediatament abans de jugar (per evitar precomputacions de nparell i nsenar amb el mateix hash(n)). Un cop s'intercanvien els hash, comparteixen el nombre triat i cada jugador valida el hash rebut amb el hash ~~del~~ del nombre de l'altre jugador. Si és el mateix valor, no ha fet trampes i podem validar a + b.

(6)

K Ferran → Vàlid, ho ha signat Alicia

K Cristina → Vàlid, ho ha signat Alicia

K Gaia → Validesa marginal, ho ha signat Ferran, que té confiança marginal ⇒ validesa total

K Daniel → Validesa marginal, ho ha signat Cristina, que té confiança marginal ⇒ validesa total

K Esteban → No té validesa, Gaia ni Daniel tenen validesa ni confiança.

(7)

La dificultat per desxifrar un sistema RSA sense conèixer les claus privades està en la dificultat de factoritzar un nombre molt gran n, $(p \cdot q)$. S'ha de provar un nombre de combinacions computacionalment enorme per a obtenir els nombres primers p i q, i així obtenir el nombre ϕ i d, per obtenir la clau privada i fer-se passar per un altre usuari.

(8) Sistema homomòrfic additiu → $E(m_1) \cdot E(m_2) = E(m_1 + m_2)$

tenim: $c_1 = Encrypt(23)$

$c_2 = Encrypt(2) \cdot c_1 = Encrypt(23+2) = Encrypt(25)$

Si Bernardo desencripta c_2, obtindrà 25

(9) L'atacant veu que s'envien els missatges:

$c_1 = k_A \oplus m$ $\quad c_2 = k_D \oplus k_A \oplus m$ $\quad c_3 = k_B \oplus m$

Amb operacions XOR sobre els missatges del canal es pot obtenir m → $m = c_1 \oplus c_2 \oplus c_3$

Les inseguer fer servir XOR

(10)

Alicia		Bernardo
$A = g^a \bmod p = 44^3 \bmod 1291 = 1269$	→ A	
B	←	$B = g^b \bmod p = 44^5 \bmod 1291 = 11$
$K = B^a = g^{ab} \bmod p = 11^3 = 40$		$K = A^b \bmod p = g^{ba} = 40$

K