

Facultat d'Informàtica de Barcelona
Examen final de Criptografia
21 de juny de 2002

Qüestió 1. Una funció hash és fortament lliure de col·lisions si és computacionalment impossible trobar un parell m i m' tal que $h(m) = h(m')$.

Suposeu que teniu $h_1 : \mathbf{Z}_2^{2\ell} \rightarrow \mathbf{Z}_2^\ell$, és a dir, una funció que transforma paraules binàries de longitud 2ℓ en paraules de longitud ℓ , i que h_1 és fortament lliure de col·lisions. Ara, si m és un missatge de longitud 4ℓ , l'escriuiu com a concatenació $m = m_1 || m_2$ de 2 de longitud 2ℓ i definiu

$$h_2(m) = h_1(h_1(m_1) || h_1(m_2))$$

Proveu que $h_2 : \mathbf{Z}_2^{4\ell} \rightarrow \mathbf{Z}_2^\ell$ és també fortament lliure de col·lisions.

SOLUCIÓ: h_2 transforma paraules binàries de longitud 4ℓ en paraules de longitud ℓ . Suposem que no fós fortament lliure de col·lisions. Es podrien trobar *de manera fàcil* missatges diferents m i m' tals que $h_2(m) = h_2(m')$. Aquests missatges de longitud 4ℓ els escrivim com a concatenació de dos de longitud 2ℓ :

$$\begin{aligned} m &= m_1 || m_2 \\ m' &= m'_1 || m'_2 \end{aligned}$$

Aleshores, $h_1(h_1(m_1) || h_1(m_2)) = h_1(h_1(m'_1) || h_1(m'_2))$. Si

$$h_1(m_1) || h_1(m_2) \neq h_1(m'_1) || h_1(m'_2)$$

hauríem trobat *de manera fàcil* missatges $x = h_1(m_1) || h_1(m_2)$ i $x' = h_1(m'_1) || h_1(m'_2)$ tals que $h_1(x) = h_1(x')$, cosa que contradiu que h_1 sigui fortament lliure de col·lisions. D'altra banda, si

$$h_1(m_1) || h_1(m_2) = h_1(m'_1) || h_1(m'_2)$$

això clarament vol dir que $h_1(m_1) = h_1(m'_1)$ i $h_1(m_2) = h_1(m'_2)$. Atès que $m \neq m'$, tindrem $m_1 \neq m'_1$ o $m_2 \neq m'_2$. En qualsevol cas, novament es contradiu el fet que h_1 sigui fortament lliure de col·lisions.

L'expressió *de manera fàcil* vol dir *amb un algoritme eficient*. Hem fet servir que trencar una cadena binària per la meitat és fàcil i que, per la mateixa definició de funció hash, el càlcul de h_1 es pot fer de manera eficient.

Qüestió 2. Suposeu que en un sistema RSA dos usuaris comparteixen el mateix mòdul n i tenen exponents públics e_1, e_2 relativament primers. Demostreu que si s'envia a tots dos un mateix missatge xifrat, aleshores qui intercepti els criptogrames podrà recuperar fàcilment el missatge original.

SOLUCIÓ: Qui intercepti els criptogrames disposarà de les quantitats

$$\begin{aligned}c_1 &= m^{e_1} \pmod n \\c_2 &= m^{e_2} \pmod n\end{aligned}$$

on m és el missatge comú, pensat ja com a enter mòdul n . Si e_1 i e_2 són relativament primers, pot trobar solucions x, y de la identitat de Bézout

$$e_1x + e_2y = 1$$

per exemple amb l'algoritme d'Euclides extès, que és eficient. Tot seguit calcula

$$\begin{aligned}s_1 &= c_1^x \pmod n \\s_2 &= c_2^y \pmod n\end{aligned}$$

amb l'algoritme de quadrats successius, que també és eficient. Finalment, fent el producte

$$s_1s_2 \pmod n$$

recupera el missatge:

$$s_1s_2 \pmod n = c_1^x c_2^y \pmod n = m^{e_1x + e_2y} \pmod n = m^1 \pmod n = m \pmod n = m$$

Qüestió 3. Avantatges i inconvenients de l'ús de criptosistemes basats en corbes el·líptiques.

SOLUCIÓ: Els punts més significatius són:

- L'operació de grup (suma de punts) és més complicada que el producte de números enters.
- El càlcul del cardinal del grup es costós.
- Amb un mateix primer p (mateixa aritmètica modular) es poden plantejar diferents criptosistemes, canviant els coeficients de la corba.
- No es coneixen algorismes subexponencials per resoldre el logaritme discret en el grup de punts d'una corba el·líptica sobre un cos finit. Per tant, s'aconsegueixen els mateixos nivells de seguretat treballant amb primers més petits.

Qüestió 4. Què fa i per a què serveix una autoritat certificadora?

SOLUCIÓ: Les possibilitats de redacció són molt diverses, però sembla imprescindible citar la criptografia de clau pública, la signatura digital, els certificats, l'emissió/revocació de certificats i la necessitat dels certificats per donar validesa (per exemple, legal) a la signatura digital.

(Cada qüestió val 1.5 punts. El màxim de paper que es pot entregar és d'un full per qüestió)