Crittografia ed Aritmetica Modulare
LABORATORIO del VI incontro

PLS - CAM

Padova, 21 novembre 2014

Ricordiamo dapprima i tre importanti risultati della prima sezione:

Teorema 1.1 (PICCOLO TEOREMA DI FERMAT)**.** *Sia p un intero primo e sia $\overline{0} \neq \overline{a} \in \mathbb{Z}_p$. Allora*

$$\overline{a}^{\,p-1} = \overline{1} \quad in \quad \mathbb{Z}_p.$$

Corollario1.2. *Sia p un intero primo e sia $a \in \mathbb{Z}$. Allora*

$$a^p \equiv a \mod p.$$

Teorema 1.3 (TEOREMA DI EULERO-FERMAT)**.** *Sia n un arbitrario intero positivo e sia $\overline{a}$ invertibile in $\mathbb{Z}_n$. Allora $\overline{a}^{\,\varphi(n)} = \overline{1}$ in $\mathbb{Z}_n$.*

ATTIVITÀ 1.4. *Alcune semplici riflessioni sui precedenti risultati.*

- *Il Piccolo Teorema di Fermat è un immediato corollario del Teorema di Eulero-Fermat. Infatti ...*
- *Il* Corollario 1.2 *è di fatto del tutto equivalente al* Teorema 1.1. *Assumete come ipotesi l'enunciato di* 1.2 *e fornite una dimostrazione di* 1.1.

HOMEWORK 1.5. *Seguendo la stessa linea dimostrativa del* Piccolo Teorema di Fermat, *con $\varphi(n)$ in luogo di $p-1$, si dimostri il* Teorema di Eulero-Fermat.

Ricordiamo ora la fondamentale applicazione dei precedenti risultati al metodo RSA:

Corollario 2.1. *Sia $n = p_1\, p_2\, \ldots, p_t$, con p_i interi primi* **distinti**. *Siano e, f interi positivi tali che $ef \equiv 1 \mod \varphi(n)$. Allora*

$$\overline{a}^{\,ef} = \overline{a} \quad in \quad \mathbb{Z}_n$$

qualunque sia $\overline{a} \in \mathbb{Z}_n$.

ATTIVITÀ 2.3. *Siamo sicuri che a messaggi distinti corrispondano versioni cifrate distinte? In altre parole, l'applicazione*

$$\mathbb{Z}_n \to \mathbb{Z}_n, \quad \overline{X} \mapsto \overline{X}^{\,e}$$

è iniettiva?

ATTIVITÀ 2.4. *Proviamo ad applicare il metodo descritto nel* Corollario RSA *ad un caso estremamente semplice. Supponiamo di voler cifrare/decifrare in modo monoalfabetico (cioè carattere per carattere) un testo privo di spazi, associando ad ogni lettera dell'alfabeto italiano la sua posizione d'ordine.*

- *I caratteri sono identificati con una classe di $\mathbb{Z}_n$, con $n = 21$.*
- *In questo caso $\varphi(n) = \varphi(21) = \varphi(3 \cdot 7) = 2 \cdot 6 = 12$. Si scelga $1 < e < 12$ con $(12, e) = 1$. Sia $1 < f < 12$ tale che $ef \equiv 1 \mod 12$ (NB: qui accade sempre che $e = f$!)*
- *Si scelga un testo italiano privo di spazi, e lo si codifichi carattere per carattere applicando $\overline{X} \mapsto \overline{X}^{\,e}$.*
- *Si applichi $\overline{Y} \mapsto \overline{Y}^{\,f}$ ai caratteri del testo in codice per riottenere il testo in chiaro.*

ATTIVITÀ 3.1. *Supponiamo che siano assegnati sia n (= intero prodotto di due primi) che m (= numero dei caratteri dell'alfabeto). Qual è la massima lunghezza l (= numero dei caratteri) di una stringa che possa interpretarsi in modo univoco come scrittura m-aria di una classe $\overline{X} \in \mathbb{Z}_n$?* (Sugg.: con l cifre in $\mathbb{Z}_m$ si riescono a rappresentare esattamente m^l numeri interi ...)

Supponiamo ad esempio che n sia un numero con 500 cifre decimali e che abbiamo scelto di rappresentare i caratteri del nostro alfabeto attraverso il loro codice ASCII (cioè $m = 256$). Qual è allora la massima lunghezza di un testo traducibile in un'unica classe $\overline{X} \in \mathbb{Z}_n$?