

TRENTO, A.A. 2007/08
CAMPI FINITI E CRITTOGRAFIA SIMMETRICA
ESERCIZI

LE REGOLE

All'esame vi chiederò di svolgere

- (1) in ogni caso l'esercizio 1,
- (2) altri tre esercizi fra altri cinque di quelli seguenti che vi indicherò, e
- (3) un ulteriore esercizio, a vostra libera scelta, fra tutti gli esercizi non ancora svolti.

Se un esercizio A richiede il risultato di un altro esercizio B, è necessario e sufficiente citare il risultato dell'esercizio B.

GLI ESERCIZI

L'esercizio fondamentale.

Esercizio 1. Si dia una descrizione generale della struttura di Rijndael, indicando in particolare:

- Come venga utilizzato e rappresentato $\mathbf{GF}(2^8)$.
- Come venga rappresentato un byte.
- Come venga rappresentato un vettore di 4 bytes mediante un polinomio, e come si effettui la moltiplicazione fra queste espressioni.
- Cosa sia lo Stato, e di quanti bytes sia composto.
- Quali siano le componenti di un round tipico, e le si descrivano.
- In che modo differisca il primo round, e perché.

Altri esercizi.

Esercizio 2. Si mostri che il gruppo moltiplicativo di un campo finito è ciclico. (Comprende la citazione di tutti i risultati preparatori necessari, e la dimostrazione della formula $n = \sum_{d|n} \varphi(d)$.)

Esercizio 3. Sia \mathbf{N} l'insieme dei numeri interi positivi. Si definisca una funzione $\mu : \mathbf{N} \rightarrow \mathbf{Z}$ mediante la formula

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } n > 1. \end{cases}$$

- Si mostri che μ è univocamente determinata dalla formula precedente.
- Si mostri che μ è moltiplicativa nel senso della teoria dei numeri, ovvero $\mu(nm) = \mu(n)\mu(m)$ se $(n, m) = 1$.

- Si mostri che

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se esiste un primo } p \text{ tale che } p^2 \mid n, \\ (-1)^k & \text{se } n \text{ è il prodotto di } k \text{ primi distinti.} \end{cases}$$

Esercizio 4. Si dimostri la formula di inversione di Moebius, cioè che se $f, g : \mathbf{N} \rightarrow \mathbf{C}$, e $g(n) = \sum_{d|n} f(d)$, allora $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$.

Esercizio 5. Si descrivano i sottogruppi di un gruppo ciclico di ordine n finito.

(SUGGERIMENTO: Si tratta di far vedere che ce n'è uno e uno solo di ordine d , per ogni divisore d di n .)

Esercizio 6. Si mostri che $\mathbf{GF}(p^d) \subseteq \mathbf{GF}(p^n)$ se e solo se d divide n ,

- sia mediante la corrispondenza di Galois,
- sia mostrando che $x^{p^d} - x$ divide $x^{p^n} - x$ se e solo se d divide n .

Esercizio 7. Sia p un primo, e n un intero positivo. Si mostri che $x^{p^n} - x \in \mathbf{F}_p[x]$ è il prodotto di tutti i polinomi monici e irriducibili distinti di $\mathbf{F}_p[x]$, di grado un divisore di n .

Esercizio 8. Discutere la crittanalisi delle trasformazioni affini rispetto ad attacchi:

- chosen plaintext,
- given plaintext.

Esercizio 9. Si dia la formula per il numero di polinomi (monici e) irriducibili di grado n sul campo con p elementi, ove p è un numero primo. Si dica quanti di essi sono primitivi.

Esercizio 10. Si consideri il polinomio $m = x^8 + x^4 + x^3 + x + 1 \in \mathbf{F}_2[x]$ di Rijndael.

Si mostri che m è irriducibile in $\mathbf{F}_2[x]$.

Esercizio 11. Sia $E = \mathbf{GF}(2^8)$, Si trovi l'inverso in $E[x]$ del polinomio

$$c = (\alpha + 1)x^3 + x^2 + x + \alpha$$

modulo $x^4 + 1$. Qui α è una radice di m (vedi Esercizio 10).

Esercizio 12. Si dimostri il singleton bound per un codice lineare su un campo finito F qualsiasi.

(SUGGERIMENTO: Si tratta quindi di mostrare che se il codice lineare \mathcal{C} (sottospazio dello spazio F^n) ha dimensione k , e distanza minima d , allora $d \leq n - k + 1$.)

Esercizio 13. Sia $E = \mathbf{GF}(2^n)$. Sia $F : E \rightarrow E$ la funzione inversione $x \mapsto x^{-1}$, con la convenzione che $0^{-1} = 0$.

Si descriva la propagazione delle differenze attraverso F : in altre parole, si dica, per $0 \neq \beta \in E$ fissato, quanti valori assume la funzione

$$f : E \rightarrow E \\ x \mapsto x^{-1} + (x + \beta)^{-1},$$

(cioè qual è la cardinalità dell'immagine di f), e quante volte viene assunto ogni valore (cioè per $y \in E$ fissato, quanti $x \in E$ ci sono tali che $f(x) = f(y)$).

Esercizio 14. Sia F un campo finito di ordine 2^n , e sia $f = x^2 + ax + b \in F[x]$. Si dica quando f ha radici in F , e si dimostri quanto affermato.

Esercizio 15. Sia α una radice di m (vedi Esercizio 10). Si consideri la matrice

$$A = \begin{bmatrix} \alpha & \alpha + 1 & 1 & 1 \\ 1 & \alpha & \alpha + 1 & 1 \\ 1 & 1 & \alpha & \alpha + 1 \\ \alpha + 1 & 1 & 1 & \alpha \end{bmatrix}.$$

Si mostri che ogni minore di A è diverso da zero.

Esercizio 16. Sia \mathcal{C} un codice lineare di dimensione k in E^n , ove E è un campo finito. Sia H la sua matrice di controllo di parità. Si enunci la condizione su H affinché la distanza minima di \mathcal{C} sia (almeno) d .

Si mostri che la matrice 4×8 a blocchi

$$H = [A \mid 1],$$

ove A è la matrice dell'Esercizio 15, definisce un codice $[8, 4, 5]$ su $E = \mathbf{GF}(2^8)$.

Esercizio 17. Si mostri che il *branch number* della trasformazione $v \mapsto A \cdot v$ è 5. Qui A è come nell'Esercizio 15, e $v \in E^4$ è un vettore colonna, con $E = \mathbf{GF}(2^8)$.

(SUGGERIMENTO: Il branch number di A è il minimo (al variare di v fra gli elementi non nulli di E^4) della somma fra il numero di bytes non nulli di v più il numero di bytes non nulli di Av .)

Esercizio 18. Enunciare e dimostrare il teorema della 25 S-box attive su 4 rounds.

Esercizio 19. Si enunci e si dimostri l'espressione per la distanza di una funzione dall'insieme delle funzioni affini in termini di correlazioni con le funzioni lineari.

Esercizio 20. Sia $E = \mathbf{GF}(2^m)$. Si enunci e dimostri il bound per la distanza della funzione inversione su E dalle funzioni affini.

Esercizio 21. Sia ρ un round di AES, che opera su $V = \mathbf{F}_2^{128}$. Si mostri che non esiste un sottospazio $U \neq \{0\}$, V tale che per ogni $u \in U$ e $x \in V$ si abbia

$$\rho(x + u) - \rho(x) \in U.$$