Campi Finiti
e Applicazioni

Luca Amata

Università degli Studi di Messina

Seminario
per Laurea Triennale in Matematica

Dicembre 2018

Introduzione

Il seminario si divide in due blocchi:

- **Campi Finiti**
  - Teoremi di esistenza e unicità
  - Costruzione
  - Gruppo moltiplicativo
  - Sottocampi
  - Polinomi irriducibili
- **Crittografia**
  - Protocollo asimmetrico di *Diffie-Hellman*
  - Sistema di *ElGamal* (logaritmo discreto)
  - Curve Ellittiche

Introduzione

Il seminario si divide in due blocchi:

- **Campi Finiti**
  - Teoremi di esistenza e unicità
  - Costruzione
  - Gruppo moltiplicativo
  - Sottocampi
  - Polinomi irriducibili
- **Crittografia**
  - Protocollo asimmetrico di *Diffie-Hellman*
  - Sistema di *ElGamal* (logaritmo discreto)
  - Curve Ellittiche

Struttura dei Campi Finiti

- Sia F campo e P il suo sottocampo fondamentale
  - Se $char(F) = p$, primo, allora $P \cong \mathbb{Z}_p$
  - Se $char(F) = 0$ allora $P \cong \mathbb{Q}$
- Se F campo finito allora e
  - $char(F) = p$, p primo
  - $|F| = p^n = q$, $n \in \mathbb{N}^+$
- Dati comunque un primo p e un intero positivo n
  - Esiste un campo con $q = p^n$ elementi
  - È unico a meno di isomorfismi

  Tale campo viene identificato dal simbolo $\mathbb{F}_q$

Struttura dei Campi Finiti

- Sia F campo e P il suo sottocampo fondamentale
  - Se $char(F) = p$, primo, allora $P \cong \mathbb{Z}_p$
  - Se $char(F) = 0$ allora $P \cong \mathbb{Q}$
- Se F campo finito allora e
  - $char(F) = p$, p primo
  - $|F| = p^n = q$, $n \in \mathbb{N}^+$
- Dati comunque un primo p e un intero positivo n
  - Esiste un campo con $q = p^n$ elementi
  - È unico a meno di isomorfismi

Tale campo viene identificato dal simbolo $\mathbb{F}_q$

Struttura dei Campi Finiti

- Sia F campo e P il suo sottocampo fondamentale
  - Se $char(F) = p$, primo, allora $P \cong \mathbb{Z}_p$
  - Se $char(F) = 0$ allora $P \cong \mathbb{Q}$
- Se F campo finito allora e
  - $char(F) = p$, p primo
  - $|F| = p^n = q$, $n \in \mathbb{N}^+$
- Dati comunque un primo p e un intero positivo n
  - Esiste un campo con $q = p^n$ elementi
  - È unico a meno di isomorfismi

  Tale campo viene identificato dal simbolo $\mathbb{F}_q$

Costruzione di $\mathbb{F}_9$ (1/2)

Costruzione del campo finito con 9 elementi $\mathbb{F}_9$

- Come **campo di spezzamento** di un polinomio
  - Sia $x^9 - x \in \mathbb{Z}_3[x]$, scomposto in fattori irriducibili

    $x^9 - x = x(x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1)$
  - Considerare le rispettive radici $\mathbb{F}_9 = \{0, 1, 2, \alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2\}$
- Come **quoziente** dell'anello dei polinomi
  - $\mathbb{Z}_3[x]/(x^2+x-1) = \{a + bx \ : \ a, b \in \mathbb{Z}_3, \ \mathrm{x}^2 = -x+1\}$ campo
  - rappresentazione elementi $\{0, 1, 2, x, 1+x, 2+x, 2x, 1+2x, 2+2x\}$
  - Considerati β, α tali che $\beta^2 + \beta - 1 = 0$, $\alpha^2 + 1 = 0$, vale

    $\mathbb{Z}_3(\beta) = \mathbb{Z}_3[x]/(x^2+x-1) \cong \mathbb{Z}_3[x]/(x^2+1) = \mathbb{Z}_3(\alpha)$

    con $\varphi : \ \mathbb{Z}_3(\beta) \to \mathbb{Z}_3(\alpha)$ tale che $\beta \mapsto \alpha + 1$.

Costruzione di $\mathbb{F}_9$ (1/2)

Costruzione del campo finito con 9 elementi $\mathbb{F}_9$

- Come **campo di spezzamento** di un polinomio
  - Sia $x^9 - x \in \mathbb{Z}_3[x]$, scomposto in fattori irriducibili
    $x^9 - x = x(x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1)$
  - Considerare le rispettive radici $\mathbb{F}_9 = \{0, 1, 2, \alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2\}$
- Come **quoziente** dell'anello dei polinomi
  - $\mathbb{Z}_3[x]/(x^2+x-1) = \{a + bx \ : \ a, b \in \mathbb{Z}_3, \ \mathrm{x}^2 = -x + 1\}$ campo
  - rappresentazione elementi $\{0, 1, 2, x, 1+x, 2+x, 2x, 1+2x, 2+2x\}$
  - Considerati β, α tali che $\beta^2 + \beta - 1 = 0$, $\alpha^2 + 1 = 0$, vale
    $\mathbb{Z}_3(\beta) = \mathbb{Z}_3[x]/(x^2+x-1) \cong \mathbb{Z}_3[x]/(x^2+1) = \mathbb{Z}_3(\alpha)$
    con $\varphi : \ \mathbb{Z}_3(\beta) \to \mathbb{Z}_3(\alpha)$ tale che $\beta \mapsto \alpha + 1$.

Costruzione di $\mathbb{F}_9$ (2/2)

Con $g_1 = 0, g_2 = x, g_3 = 2x, g_4 = 1, g_5 = 1 + x, g_6 = 1 + 2x, g_7 = 2, g_8 = 2 + x, g_9 = 2 + 2x$

(GF[9], +) x + y

x \ y	g1	g2	g3	g4	g5	g6	g7	g8	g9
g1	g1	g2	g3	g4	g5	g6	g7	g8	g9
g2	g2	g3	g1	g5	g6	g4	g8	g9	g7
g3	g3	g1	g2	g6	g4	g5	g9	g7	g8
g4	g4	g5	g6	g7	g8	g9	g1	g2	g3
g5	g5	g6	g4	g8	g9	g7	g2	g3	g1
g6	g6	g4	g5	g9	g7	g8	g3	g1	g2
g7	g7	g8	g9	g1	g2	g3	g4	g5	g6
g8	g8	g9	g7	g2	g3	g1	g5	g6	g4
g9	g9	g7	g8	g3	g1	g2	g6	g4	g5

(a) Somma

(GF[9], x) x * y

x \ y	g1	g2	g3	g4	g5	g6	g7	g8	g9
g1	g1	g1	g1	g1	g1	g1	g1	g1	g1
g2	g1	g6	g8	g2	g4	g9	g3	g5	g7
g3	g1	g8	g6	g3	g7	g5	g2	g9	g4
g4	g1	g2	g3	g4	g5	g6	g7	g8	g9
g5	g1	g4	g7	g5	g8	g2	g9	g3	g6
g6	g1	g9	g5	g6	g2	g7	g8	g4	g3
g7	g1	g3	g2	g7	g9	g8	g4	g6	g5
g8	g1	g5	g9	g8	g3	g4	g6	g7	g2
g9	g1	g7	g4	g9	g6	g3	g5	g2	g8

(b) Prodotto

Figura: Tavole delle operazioni di $\mathbb{F}_9$

Automorfismi e Gruppo Moltiplicativo

- Sia F un campo di caratteristica p. La mappa $\Phi : \; F \to F$ definita da $a \mapsto a^p$ è detta **omomorfismo di Frobenius**.
  - Φ è sempre iniettivo
  - Se F è finito allora Φ è un automorfismo, $F = F^p$
  - Se $\mathbb{F}_q, \;\; q = p^n$, si ha $\Phi^r : \; a \mapsto a^{p^r}$, $r \geq 1$
- Il **Gruppo Moltiplicativo** di un campo finito $\mathbb{F}$ è ciclico.
  - Un elemento u che lo genera è detto elemento primitivo
  - Se $char(F) = p$ allora $F = \mathbb{Z}_p(u)$
  - In $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 + 1)$ la classe $1 + x$ è un elemento primitivo
  - ! In $(\mathbb{Q}^*, \cdot)$ si ha $o(-1) = 2$, ma $\mathbb{Z}$ non possiede tale elemento

Automorfismi e Gruppo Moltiplicativo

- Sia F un campo di caratteristica p. La mappa $\Phi: \; F \to F$ definita da $a \mapsto a^p$ è detta **omomorfismo di Frobenius**.
  - Φ è sempre iniettivo
  - Se F è finito allora Φ è un automorfismo, $F = F^p$
  - Se $\mathbb{F}_q, \;\; q = p^n$, si ha $\Phi^r: \; a \mapsto a^{p^r}$, $r \geq 1$

- Il **Gruppo Moltiplicativo** di un campo finito $\mathbb{F}$ è ciclico.
  - Un elemento u che lo genera è detto elemento primitivo
  - Se $char(F) = p$ allora $F = \mathbb{Z}_p(u)$
  - In $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 + 1)$ la classe $1 + x$ è un elemento primitivo
  - ! In $(\mathbb{Q}^*, \cdot)$ si ha $o(-1) = 2$, ma $\mathbb{Z}$ non possiede tale elemento

Sottocampi

Classificazione dei **Sottocampi** di un Campo Finito

- Se $m \mid n$ allora $x^{p^m} - x \mid x^{p^n} - x$
  - Ad esempio $x(x+1)(x-1) = x^3 - x \mid x^9 - x$
- K è sottocampo di Fq, $q = p^n$, se e solo se $|K| = p^m$ con $m \mid n$
  - ! Il campo $\mathbb{F}_{16}$ non ha sottocampi di cardinalità 8
- I sottocampi di $\mathbb{F}_{p^{30}}$, p primo, rispettano la seguente struttura

$$\begin{tikzcd}
 & \mathbb{F}_{p^{30}} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{F}_{p^6} \arrow[d, dash] \arrow[dr, dash] & \mathbb{F}_{p^{10}} \arrow[dl, dash] \arrow[dr, dash] & \mathbb{F}_{p^{15}} \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{F}_{p^2} \arrow[dr, dash] & \mathbb{F}_{p^3} \arrow[d, dash] & \mathbb{F}_{p^5} \arrow[dl, dash] \\
 & \mathbb{F}_p &
\end{tikzcd}$$

Sottocampi

Classificazione dei **Sottocampi** di un Campo Finito

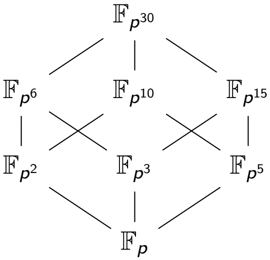
- Se $m \mid n$ allora $x^{p^m} - x \mid x^{p^n} - x$
  - Ad esempio $x(x+1)(x-1) = x^3 - x \mid x^9 - x$
- K è sottocampo di Fq, $q = p^n$, se e solo se $|K| = p^m$ con $m \mid n$
  - ! Il campo $\mathbb{F}_{16}$ non ha sottocampi di cardinalità 8
- I sottocampi di $\mathbb{F}_{p^{30}}$, p primo, rispettano la seguente struttura

$$
\begin{tikzcd}
 & \mathbb{F}_{p^{30}} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{F}_{p^6} \arrow[d, dash] \arrow[dr, dash] & \mathbb{F}_{p^{10}} \arrow[dl, dash] \arrow[dr, dash] & \mathbb{F}_{p^{15}} \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{F}_{p^2} \arrow[dr, dash] & \mathbb{F}_{p^3} \arrow[d, dash] & \mathbb{F}_{p^5} \arrow[dl, dash] \\
 & \mathbb{F}_p &
\end{tikzcd}
$$

Sottocampi

Classificazione dei **Sottocampi** di un Campo Finito

- Se $m \mid n$ allora $x^{p^m} - x \mid x^{p^n} - x$
  - Ad esempio $x(x+1)(x-1) = x^3 - x \mid x^9 - x$
- K è sottocampo di Fq, $q = p^n$, se e solo se $|K| = p^m$ con $m \mid n$
  - ! Il campo $\mathbb{F}_{16}$ non ha sottocampi di cardinalità 8
- I sottocampi di $\mathbb{F}_{p^{30}}$, p primo, rispettano la seguente struttura



Polinomi Irriducibili

Classificazione dei **Polinomi Irriducibili** su un Campo Finito

- In $\mathbb{F}_p[x]$ si ha $x^{p^n} - x = \prod p(x)$ al variare di tutti i polinomi monici $p(x)$ irriducibili su F_p di grado m tale che $m \mid n$
  - $x^9 - x \in \mathbb{Z}_3[x]$ si decompone in $\mathbb{Z}_3[x]$ come

    $$x^9 - x = x(x^8 - 1) = x(x^4 - 1)(x^4 + 1) =$$
    $$= x(x^2 - 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1) =$$
    $$= x(x - 1)(x + 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1).$$

- In $\mathbb{F}_{81}$ considerare il numero delle radici dei polinomi
  - $x^{80} - 1$ ha 80 radici
  - $x^{81} - 1$ ha 1 radice
  - $x^{88} - 1$ ha 8 radici

Polinomi Irriducibili

Classificazione dei **Polinomi Irriducibili** su un Campo Finito

- In $\mathbb{F}_p[x]$ si ha $x^{p^n} - x = \prod p(x)$ al variare di tutti i polinomi monici $p(x)$ irriducibili su F_p di grado m tale che $m \mid n$
  - $x^9 - x \in \mathbb{Z}_3[x]$ si decompone in $\mathbb{Z}_3[x]$ come

    $$x^9 - x = x(x^8 - 1) = x(x^4 - 1)(x^4 + 1) =$$
    $$= x(x^2 - 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1) =$$
    $$= x(x - 1)(x + 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1).$$

- In $\mathbb{F}_{81}$ considerare il numero delle radici dei polinomi
  - $x^{80} - 1$ ha 80 radici
  - $x^{81} - 1$ ha 1 radice
  - $x^{88} - 1$ ha 8 radici

Crittografia

La **Crittografia**, *scrittura nascosta*: comunicare con sicurezza.

- Parleremo di sistemi crittografici caratterizzati da
  - Un *algoritmo*, noto, per codificare/decodificare
  - Alcune Chiavi
- Simmetrici
  - La Chiave di codifica/decodifica è unica
  - ! Serve un metodo sicuro per scambiare la Chiave
- Asimmetrici
  - La Chiave pubblica serve per la codifica
  - La Chiave privata serve per la decodifica

Crittografia

La **Crittografia**, *scrittura nascosta*: comunicare con sicurezza.

- Parleremo di sistemi crittografici caratterizzati da
  - Un *algoritmo*, noto, per codificare/decodificare
  - Alcune Chiavi
- Simmetrici
  - La Chiave di codifica/decodifica è unica
  - ! Serve un metodo sicuro per scambiare la Chiave
- Asimmetrici
  - La Chiave pubblica serve per la codifica
  - La Chiave privata serve per la decodifica

Crittografia

La **Crittografia**, *scrittura nascosta*: comunicare con sicurezza.

- Parleremo di sistemi crittografici caratterizzati da
  - Un *algoritmo*, noto, per codificare/decodificare
  - Alcune Chiavi
- Simmetrici
  - La Chiave di codifica/decodifica è unica
  - ! Serve un metodo sicuro per scambiare la Chiave
- Asimmetrici
  - La Chiave pubblica serve per la codifica
  - La Chiave privata serve per la decodifica

Complessità Computazionale

La complessità computazionale studia le risorse minime necessarie (tempo e memoria) per la risoluzione di un problema (algoritmo)

- Problemi risolvibili in un tempo **polinomiale** T_r
  - $T_r \leq an^b$, per certi $a \in \mathbb{R}_{>0}$, $b \in \mathbb{R}_{>1}$ e $n \in \mathbb{N}$ (istanza iniziale)
  - Tali problemi sono detti *trattabili*
- Problemi risolvibili in un tempo **esponenziale** T_r
  - $T_r \leq ab^n$, per certi $a \in \mathbb{R}_{>0}$, $b \in \mathbb{R}_{>1}$ e $n \in \mathbb{N}$ (istanza iniziale)
  - ! Tali problemi sono detti *intrattabili*
- Il problema del **logaritmo discreto**
  - Gruppo $G(+) = \langle g \rangle$, $|G| = n$, sia $h \in G$
  - ? trovare $t \in \mathbb{Z}_n$ tale che $h = tg$, $t = \log_g h$
  - Se $G = \mathbb{Z}_n$ tale problema è trattabile (Euclide)
  - ! Esistono Gruppi per cui tale problema è intrattabile

Complessità Computazionale

La complessità computazionale studia le risorse minime necessarie (tempo e memoria) per la risoluzione di un problema (algoritmo)

- Problemi risolvibili in un tempo **polinomiale** T_r
  - $T_r \leq an^b$, per certi $a \in \mathbb{R}_{>0}$, $b \in \mathbb{R}_{>1}$ e $n \in \mathbb{N}$ (istanza iniziale)
  - Tali problemi sono detti *trattabili*
- Problemi risolvibili in un tempo **esponenziale** T_r
  - $T_r \leq ab^n$, per certi $a \in \mathbb{R}_{>0}$, $b \in \mathbb{R}_{>1}$ e $n \in \mathbb{N}$ (istanza iniziale)
  - ! Tali problemi sono detti *intrattabili*
- Il problema del **logaritmo discreto**
  - Gruppo $G(+) = \langle g \rangle$, $|G| = n$, sia $h \in G$
  - ? trovare $t \in \mathbb{Z}_n$ tale che $h = tg$, $t = \log_g h$
  - Se $G = \mathbb{Z}_n$ tale problema è trattabile (Euclide)
  - ! Esistono Gruppi per cui tale problema è intrattabile

Complessità Computazionale

La complessità computazionale studia le risorse minime necessarie (tempo e memoria) per la risoluzione di un problema (algoritmo)

- Problemi risolvibili in un tempo **polinomiale** T_r
  - $T_r \leq an^b$, per certi $a \in \mathbb{R}_{>0}$, $b \in \mathbb{R}_{>1}$ e $n \in \mathbb{N}$ (istanza iniziale)
  - Tali problemi sono detti *trattabili*
- Problemi risolvibili in un tempo **esponenziale** T_r
  - $T_r \leq ab^n$, per certi $a \in \mathbb{R}_{>0}$, $b \in \mathbb{R}_{>1}$ e $n \in \mathbb{N}$ (istanza iniziale)
  - ! Tali problemi sono detti *intrattabili*
- Il problema del **logaritmo discreto**
  - Gruppo $G(+) = \langle g \rangle$, $|G| = n$, sia $h \in G$
  - ? trovare $t \in \mathbb{Z}_n$ tale che $h = tg$, $t = \log_g h$
  - Se $G = \mathbb{Z}_n$ tale problema è trattabile (Euclide)
  - ! Esistono Gruppi per cui tale problema è intrattabile

Protocollo di Diffie-Hellman

Il **protocollo di Diffie-Hellman** è asimmetrico

- Noto l'algoritmo e le funzioni φ, ψ, la comunicazione avviene:
  - Chiave pubblica k resa disponibile dal proprietario
  - La funzione di codifica φ cifra il messaggio: $c = \varphi(m, k)$
  - ! φ "computazionalmente difficile" da invertire (*one-way*)
  - ! φ invertibile con informazioni addizionali (*trapdoor-one-way*)
  - La chiave privata s permette, tramite ψ, la decodifica $m = \psi(c, s)$

Bob invia un messaggio ad Alice, Eve prova a leggerlo

Protocollo di Diffie-Hellman

Il **protocollo di Diffie-Hellman** è asimmetrico

- Noto l'algoritmo e le funzioni φ, ψ, la comunicazione avviene:
  - Chiave pubblica k resa disponibile dal proprietario
  - La funzione di codifica φ cifra il messaggio: $c = \varphi(m, k)$
  - ! φ "computazionalmente difficile" da invertire (*one-way*)
  - ! φ invertibile con informazioni addizionali (*trapdoor-one-way*)
  - La chiave privata s permette, tramite ψ, la decodifica $m = \psi(c, s)$

Bob invia un messaggio ad Alice, Eve prova a leggerlo

$m = \psi(c, s)$  $\xleftarrow{\quad c \quad}$  $c = \varphi(m, k)$

k (m)

???

Sistema di ElGamal (1/3)

Il **Sistema di ElGamal** implementa il protocollo di Diffie-Hellman
(la funzione trapdoor-one-way è legata al DLP)

- È necessario fissare i seguenti elementi
  - Gruppo ciclico G di ordine n
  - Una funzione $f: \; G \longrightarrow \{0,1\}^r$ (stringhe binarie di lunghezza r)

Parametri:

- Alice sceglie un generatore del gruppo g ($\langle g \rangle = G$)
- Sceglie un intero casuale a tale che $1 \leq a \leq n-1$
- La coppia (ag, a) rappresenta la coppia di chiavi (pubblica, privata)
- Pubblica i parametri per la comunicazione: $(G, +, f, g, ag)$

Sistema di ElGamal (1/3)

Il **Sistema di ElGamal** implementa il protocollo di Diffie-Hellman
(la funzione trapdoor-one-way è legata al DLP)

- È necessario fissare i seguenti elementi
  - Gruppo ciclico G di ordine n
  - Una funzione $f: \ G \longrightarrow \{0,1\}^r$ (stringhe binarie di lunghezza r)

Parametri:

- Alice sceglie un generatore del gruppo g ($\langle g \rangle = G$)
- Sceglie un intero casuale a tale che $1 \leq a \leq n-1$
- La coppia (ag, a) rappresenta la coppia di chiavi (pubblica, privata)
- Pubblica i parametri per la comunicazione: $(G, +, f, g, ag)$

Sistema di ElGamal (2/3)

Codifica:

- Bob vuole inviare il messaggio $m \in \{0,1\}^r$ ad Alice
- Sceglie un intero casuale b tale che $1 \leq b \leq n-1$
- Calcola bg e codifica il messaggio: $c = m + f(b(ag))$
- Invia ad Alice la coppia (bg, c)

Decodifica:

- Alice riceve (bg, c)
- Osserva che $a(bg) = (ab)g = (ba)g = b(ag)$
- Calcola $m = c - f(b(ag))$, messaggio non cifrato

Intercettazione:

- ???

Sistema di ElGamal (2/3)

Codifica:

- Bob vuole inviare il messaggio $m \in \{0,1\}^r$ ad Alice
- Sceglie un intero casuale b tale che $1 \leq b \leq n-1$
- Calcola bg e codifica il messaggio: $c = m + f(b(ag))$
- Invia ad Alice la coppia (bg, c)

Decodifica:

- Alice riceve (bg, c)
- Osserva che $a(bg) = (ab)g = (ba)g = b(ag)$
- Calcola $m = c - f(b(ag))$, messaggio non cifrato

Intercettazione:

- ???

Sistema di ElGamal (2/3)

Codifica:

- Bob vuole inviare il messaggio $m \in \{0,1\}^r$ ad Alice
- Sceglie un intero casuale b tale che $1 \leq b \leq n-1$
- Calcola bg e codifica il messaggio: $c = m + f(b(ag))$
- Invia ad Alice la coppia (bg, c)

Decodifica:

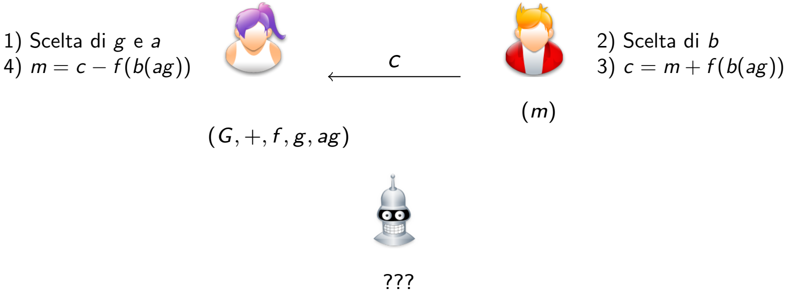
- Alice riceve (bg, c)
- Osserva che $a(bg) = (ab)g = (ba)g = b(ag)$
- Calcola $m = c - f(b(ag))$, messaggio non cifrato

Intercettazione:

- ???

Sistema di ElGamal (3/3)

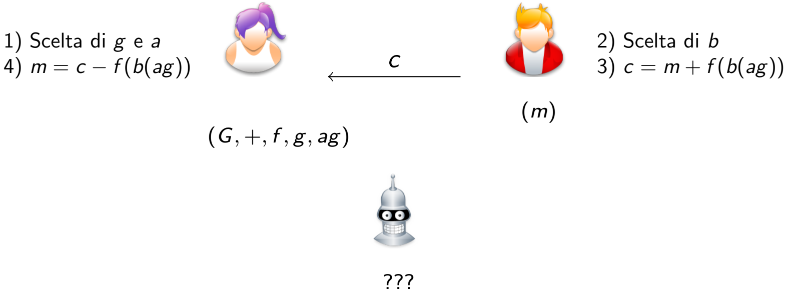
Schema della comunicazione



- Considerazioni:
  - Tale sistema è sicuro fintanto che il DLP (ottenere a da ag e b da bg senza chiavi) è intrattabile
  - La *chiave* di codifica/decodifica è $b(ag)$ che Alice e Bob possiedono

Sistema di ElGamal (3/3)

Schema della comunicazione



- Considerazioni:
  - Tale sistema è sicuro fintanto che il DLP (ottenere a da ag e b da bg senza chiavi) è intrattabile
  - La *chiave* di codifica/decodifica è $b(ag)$ che Alice e Bob possiedono

Curve Ellittiche (1/3)

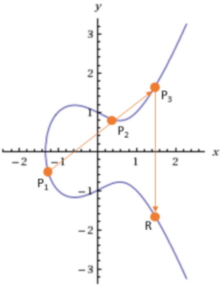
- Proprietà geometriche di una **Curva Ellittica** E sul campo $\mathbb{F}_q$:
  - *Forma di Weierstrass*: $E/\mathbb{F}_q : \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ dove $a_i \in \mathbb{F}_q$ e il discriminante è non nullo.
  - Sia $\mathrm{Supp}(E) \subset \mathbb{F}_q \times \mathbb{F}_q$ il supporto
  - Sia $\mathcal{O}$ il punto proiettivo di E
  - Si definisca l'insieme $E(\mathbb{F}_q) := \mathrm{Supp}(E) \cup \mathcal{O}$
- $(E(\mathbb{F}_q), +)$ è un gruppo abeliano con elemento neutro $\mathcal{O}$.
  Siano $P_1, P_2 \in E(\mathbb{F}_q)$, si definisce $P_1 + P_2 := R \in E(\mathbb{F}_q)$:
  - tracciare la retta r passante per essi
  - individuare il terzo punto di intersezione $r \cap E$, sia esso P_3
  - tracciare la retta s passante per P_3 e $\mathcal{O}$
  - individuare il terzo punto di intersezione $s \cap E$, sia esso R

Curve Ellittiche (1/3)

- Proprietà geometriche di una **Curva Ellittica** E sul campo $\mathbb{F}_q$:
  - *Forma di Weierstrass*: $E/\mathbb{F}_q: \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ dove $a_i \in \mathbb{F}_q$ e il discriminante è non nullo.
  - Sia $\mathrm{Supp}(E) \subset \mathbb{F}_q \times \mathbb{F}_q$ il supporto
  - Sia $\mathcal{O}$ il punto proiettivo di E
  - Si definisca l'insieme $E(\mathbb{F}_q) := \mathrm{Supp}(E) \cup \mathcal{O}$
- $(E(\mathbb{F}_q), +)$ è un gruppo abeliano con elemento neutro $\mathcal{O}$.
  Siano $P_1, P_2 \in E(\mathbb{F}_q)$, si definisce $P_1 + P_2 := R \in E(\mathbb{F}_q)$:
  - tracciare la retta r passante per essi
  - individuare il terzo punto di intersezione $r \cap E$, sia esso P_3
  - tracciare la retta s passante per P_3 e $\mathcal{O}$
  - individuare il terzo punto di intersezione $s \cap E$, sia esso R

Curve Ellittiche (2/3)

La curva $E: \ y^2 = x^3 - x + 1$ su $\mathbb{F}_7$, non singolare con $\mathcal{O}[0,1,0]$.



$P_1 \neq P_2$

- r retta per P_1, P_2
- $P_3 = r \cap E$
- s retta per $P_3, \mathcal{O}$
- $R = s \cap E$

$P_1 = P_2$

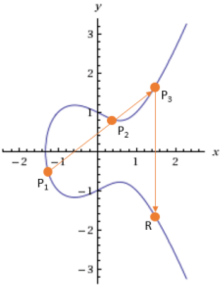
- tangente r in P_1
- $P_3 = r \cap E$
- s retta per $P_3, \mathcal{O}$
- $R = s \cap E$

$P_1 = -P_2$

- r retta per P_1, P_2
- $P_3 = r \cap E = \mathcal{O}$
- tangente s in $\mathcal{O}$
- $R = s \cap E = \mathcal{O}$

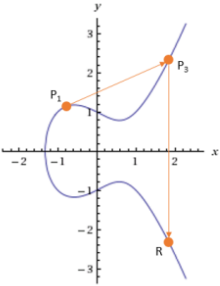
Curve Ellittiche (2/3)

La curva $E: \; y^2 = x^3 - x + 1$ su $\mathbb{F}_7$, non singolare con $\mathcal{O}[0,1,0]$.



$P_1 \neq P_2$

- r retta per P_1, P_2
- $P_3 = r \cap E$
- s retta per $P_3, \mathcal{O}$
- $R = s \cap E$



$P_1 = P_2$

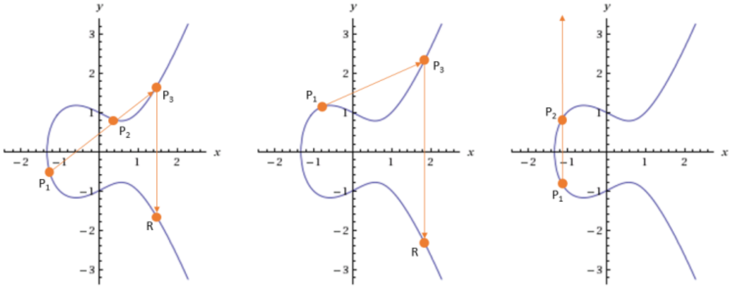
- tangente r in P_1
- $P_3 = r \cap E$
- s retta per $P_3, \mathcal{O}$
- $R = s \cap E$

$P_1 = -P_2$

- r retta per P_1, P_2
- $P_3 = r \cap E = \mathcal{O}$
- tangente s in $\mathcal{O}$
- $R = s \cap E = \mathcal{O}$

Curve Ellittiche (2/3)

La curva $E: \; y^2 = x^3 - x + 1$ su $\mathbb{F}_7$, non singolare con $\mathcal{O}[0,1,0]$.



$P_1 \neq P_2$

- r retta per P_1, P_2
- $P_3 = r \cap E$
- s retta per $P_3, \mathcal{O}$
- $R = s \cap E$

$P_1 = P_2$

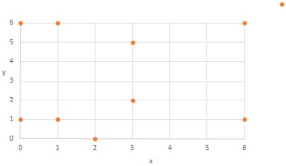
- tangente r in P_1
- $P_3 = r \cap E$
- s retta per $P_3, \mathcal{O}$
- $R = s \cap E$

$P_1 = -P_2$

- r retta per P_1, P_2
- $P_3 = r \cap E = \mathcal{O}$
- tangente s in $\mathcal{O}$
- $R = s \cap E = \mathcal{O}$

Curve Ellittiche (3/3)

Gli elementi di $E(\mathbb{F}_7)$ si possono così determinare:

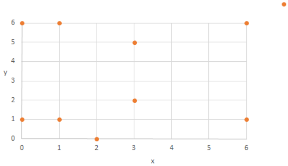


- $x = 0 \;\Rightarrow\; y^2 = 1 \;\Rightarrow\; y = 1, 6$
- $x = 3 \;\Rightarrow\; y^2 = 4 \;\Rightarrow\; y = 2, 5$
- $x = 4 \;\Rightarrow\; y^2 = 5 \;\Rightarrow\; \nexists y \in \mathbb{F}_7$

- Considerazioni sul problema del logaritmo discreto:
  - Sia $G = E(\mathbb{F}_q)$ il gruppo dei punti razionali di una curva ellittica
  - Sia q un valore abbastanza grande
  - Il problema del logaritmo discreto ha complessità esponenziale
  - Il Sistema di ElGamal su G può considerarsi sicuro

Curve Ellittiche (3/3)

Gli elementi di $E(\mathbb{F}_7)$ si possono così determinare:



- $x = 0 \Rightarrow y^2 = 1 \Rightarrow y = 1, 6$
- $x = 3 \Rightarrow y^2 = 4 \Rightarrow y = 2, 5$
- $x = 4 \Rightarrow y^2 = 5 \Rightarrow \nexists y \in \mathbb{F}_7$

- Considerazioni sul problema del logaritmo discreto:
  - Sia $G = E(\mathbb{F}_q)$ il gruppo dei punti razionali di una curva ellittica
  - Sia q un valore abbastanza grande
  - Il problema del logaritmo discreto ha complessità esponenziale
  - Il Sistema di ElGamal su G può considerarsi sicuro

Bibliografia I

T. Hungerford, *Algebra*.
No. 73 in Graduate Texts in Mathematics, New York: Springer-Verlag, 1974.

I. Herstein, *Algebra*.
University Press, Roma: Editori Riuniti, 1982.

G. Piacentini Cattaneo, *Algebra - un approccio algoritmico*.
Padova: Decibel-Zanichelli, 1996.

Z. Wan, *Lectures on Finite Fields and Galois Rings*.
World Scientific, 2003.

C. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, 1948.

I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*.
New York, NY, USA: Cambridge University Press, 1999.

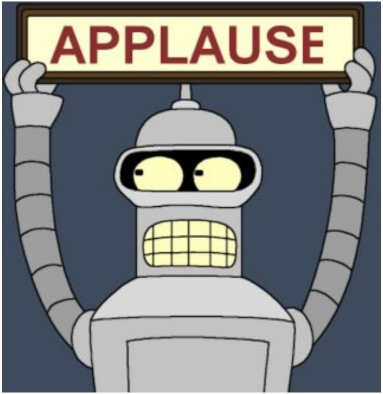
W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theor.*, vol. 22, pp. 644–654, Sept. 2006.

Bibliografia II

T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYPTO 84 on Advances in cryptology*, (New York), pp. 10–18, Springer-Verlag, 1985.

E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management - part 1: General (revised)," in *NIST Special Publication*, 2006.

Fine



Grazie per l'attenzione