Diffie-Hellman-Merkle key exchange su $\mathbb{Z}_p^*$.
Il signor Rossi e il signor Bianchi vogliono condividere un numero segreto senza inviarselo. Si accordano su un primo p e una radice primitiva $\bar{g} \in \mathbb{Z}_p^*$.
Le chiavi segrete di Rossi e Bianchi sono numeri interi a caso fra $\{2, \ldots, p-2\}$, dati rispettivamente da m_R e m_B.

Rossi spedisce a Bianchi

$$\bar{g}^{m_R} \mod p; \tag{1}$$

Bianchi riceve (1) e calcola

$$(\bar{g}^{m_R})^{m_B} \equiv \bar{g}^{m_R m_B} \mod p;$$

Bianchi spedisce a Rossi

$$\bar{g}^{m_B} \mod p; \tag{2}$$

Rossi riceve (2) e calcola

$$(\bar{g}^{m_B})^{m_R} \equiv \bar{g}^{m_B m_R} \mod p;$$

Le strighe che Rossi e Bianchi si scambiano viaggiano in chiaro e non possono essere decriptate senza risolvere il logaritmo discreto in $\mathbb{Z}_p^*$. Alla fine sono entrambi in possesso della stesso numero segreto

$$\bar{g}^{m_B m_R} \equiv \bar{g}^{m_R m_B} \mod p.$$

Esempio. Per condividere il codice del bancomat, Rossi e Bianchi si accordano sul primo $p = 1000003$ e sulla radice primitiva $\bar{2} \in \mathbb{Z}_p^*$. Le loro chiavi segrete sono interi, dati rispettivamente da $m_R = 188896$ e $m_B = 76846$.

Rossi spedisce a Bianchi

$$\bar{2}^{188896} \equiv 37008 \mod 1000003;$$

Bianchi riceve e calcola $37008^{76846} \equiv 314789 \mod 1000003$

Da parte sua Bianchi spedisce a Rossi

$$\bar{2}^{76846} \equiv 207518 \mod 1000003;$$

Rossi riceve e calcola $207518^{188896} \equiv 314789 \mod 1000003$.

Alla fine condividono il codice del bancomat 314789 senza averlo spedito direttamente. Le stringhe in viaggio 207518 e 37008 sono indecifrabili e non permettono di ricostruire il codice a meno di calcolare il logaritmo discreto di almeno una delle due.

Diffie-Hellman-Merkle key exchange su una curva ellittica.
Il signor Rossi e il signor Bianchi vogliono condividere un numero segreto senza inviarselo. Si accordano su un primo p, una curva ellittica $E(\ \mathbb{Z}_p)$ di ordine Q primo, in modo che il gruppo $(E(\ \mathbb{Z}_p), +)$ sia ciclico, e su un generatore $P = (x_0, y_0)$ di $E(\ \mathbb{Z}_p)$.
Le chiavi segrete di Rossi e Bianchi sono interi a caso fra $\{2, \ldots, Q-2\}$, dati rispettivamente da m_R e m_B.

Rossi spedisce a Bianchi

$$m_R \cdot P \in E(\ \mathbb{Z}_p); \tag{1}$$

Bianchi riceve (1) e calcola

$$m_B \cdot (m_R \cdot P) \in E(\ \mathbb{Z}_p);$$

Bianchi spedisce a Rossi

$$m_B \cdot P \in E(\ \mathbb{Z}_p); \tag{2}$$

Rossi riceve (2) e calcola

$$m_R \cdot (m_B \cdot P) \in E(\ \mathbb{Z}_p) \mod p;$$

Le stringhe che Rossi e Bianchi si scambiano viaggiano in chiaro e non possono essere decriptate senza risolvere il logaritmo discreto in $E(\ \mathbb{Z}_p)$. Alla fine sono entrambi in possesso della stesso numero segreto

$$m_B m_R \cdot P = m_R m_B \cdot P.$$

Esempio. Il signor Rossi e il signor Bianchi si accordano sulle chiavi pubbliche

$$p = 467, \quad E(\ \mathbb{Z}_p) : Y^2 = X^3 + X + 3, \quad Q = \#E(\ \mathbb{Z}_p) = 449 \text{ primo}, \quad P = (2, 78) \in E(\ \mathbb{Z}_p).$$

Le chiavi segrete di Rossi e Bianchi sono rispettivamente

$$m_R = 345, \qquad m_B = 267.$$

Rossi spedisce a Bianchi

$$m_R \cdot P = (218, 375) \in E(\ \mathbb{Z}_{467});$$

Bianchi riceve e calcola

$$m_B \cdot (218, 375) = (383, 267).$$

Bianchi spedisce a Rossi

$$m_B \cdot P = (23, 84) \in E(\ \mathbb{Z}_{467})$$

Rossi riceve e calcola

$$m_R \cdot (23, 84) = (383, 267)$$

Alla fine sono entrambi in possesso della stesso numero segreto

$$m_B m_R \cdot P = m_R m_B \cdot P = (383, 267) \in E(\ \mathbb{Z}_{467}).$$

Criptosistema a chiave pubblica ElGamal.

Il signor Rossi desidera ricevere messaggi criptati. Gli vengono fornite
chiavi pubbliche: p primo, $\bar{g}$ radice primitiva di $\mathbb{Z}_p^*$ ed un intero $E \in \mathbb{Z}_p^*$;
chiave privata: $D = \log_{\bar{g}} E$.

Supponiamo di voler inviare a Rossi il messagio m:
scegliamo a caso $\mu \in \{2, \ldots, p-2\}$ e spediamo a Rossi la coppia

$$(c_1, c_2) = (\bar{g}^{\mu}, mE^{\mu}) \mod p. \tag{3}$$

Rossi riceve (3) e calcola

$$c_2 \cdot c_1^{-D} = mE^{\mu} \cdot g^{-\mu D} = m \cdot \bar{g}^{D\mu} \cdot g^{-\mu D} \equiv m \mod p.$$

OSSERVAZIONE: Qual è il ruolo dell'esponente μ, *conosciuto solo dal mittente*? è quello di evitare che un estraneo possa calcolare m semplicemente mediante

$$m = c_2 \cdot E^{-1} \mod p.$$

Esempio. Supponiamo che le chiavi pubbliche di Rossi siano

$$p = 892785847, \quad \bar{g} = 3, \quad E = 627625155$$

e la sua chiave segreta sia

$$D = \log_{\bar{3}} E = 181997.$$

Sia $m = 30244551$ il messaggio che vogliamo inviargli, dopo averlo criptato.
Scegliamo a caso $\mu = 100028$ e inviamo a Rossi la coppia

$$(c_1, c_2) = (\bar{g}^{\mu}, m \cdot E^{\mu}) = (305987288, 47793599) \mod 892785847.$$

Rossi riceve e legge calcolando

$$m = c_2 \cdot c_1^{-D} = 30244551 \mod 892785847.$$