

# Criptografie și Securitate

- Prelegerea 23.1 -

Schimbul de chei Diffie-Hellman pe curbe eliptice

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică  
Universitatea din București

# Cuprins

1. Schimbul de chei Diffie-Hellman pe curbe eliptice
2. Securitate

# Schimbul de chei Diffie-Hellman pe curbe eliptice

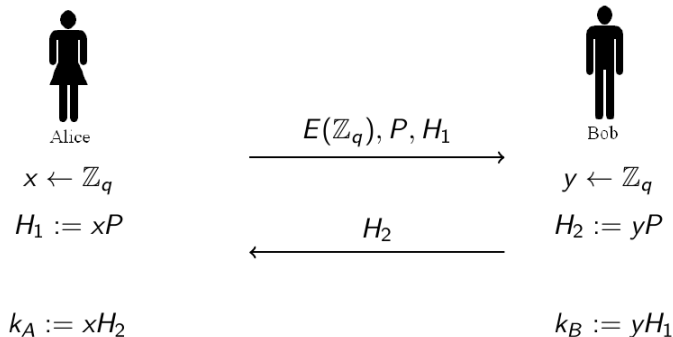
- ▶ Am studiat schimbul de chei Diffie-Hellman peste un grup ciclic  $\mathbb{G}$ , de ordin  $q$ ;

# Schimbul de chei Diffie-Hellman pe curbe eliptice

- ▶ Am studiat schimbul de chei Diffie-Hellman peste un grup ciclic  $\mathbb{G}$ , de ordin  $q$ ;
- ▶ Transpunem construcția pe curbe eliptice:

$$(\mathbb{G}, \cdot) \rightarrow (E(\mathbb{Z}_q), +)$$

# Schimbul de chei Diffie-Hellman pe curbe eliptice



# Schimbul de chei Diffie-Hellman pe curbe eliptice

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;

# Schimbul de chei Diffie-Hellman pe curbe eliptice

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;
- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$ , și  $P$  un punct pe curbă (generator);

# Schimbul de chei Diffie-Hellman pe curbe eliptice

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;
- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$ , și  $P$  un punct pe curbă (generator);
- ▶ Alice alege  $x \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H_1 := xP$ ;



# Schimbul de chei Diffie-Hellman pe curbe eliptice

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;
- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$ , și  $P$  un punct pe curbă (generator);
- ▶ Alice alege  $x \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H_1 := xP$ ;
- ▶ Alice îi trimite lui Bob mesajul  $(E(\mathbb{Z}_q), P, H_1)$ ;

# Schimbul de chei Diffie-Hellman pe curbe eliptice

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;
- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$ , și  $P$  un punct pe curbă (generator);
- ▶ Alice alege  $x \leftarrow^R \mathbb{Z}_q$  și calculează  $H_1 := xP$ ;
- ▶ Alice îi trimite lui Bob mesajul  $(E(\mathbb{Z}_q), P, H_1)$ ;
- ▶ Bob alege  $y \leftarrow^R \mathbb{Z}_q$  și calculează  $H_2 := yP$ ;

# Schimbul de chei Diffie-Hellman pe curbe eliptice

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;
- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$ , și  $P$  un punct pe curbă (generator);
- ▶ Alice alege  $x \leftarrow^R \mathbb{Z}_q$  și calculează  $H_1 := xP$ ;
- ▶ Alice îi trimite lui Bob mesajul  $(E(\mathbb{Z}_q), P, H_1)$ ;
- ▶ Bob alege  $y \leftarrow^R \mathbb{Z}_q$  și calculează  $H_2 := yP$ ;
- ▶ Bob îi trimite  $H_2$  lui Alice și întoarce cheia  $k_B := yH_1$ ;

# Schimbul de chei Diffie-Hellman pe curbe eliptice

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;
- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$ , și  $P$  un punct pe curbă (generator);
- ▶ Alice alege  $x \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H_1 := xP$ ;
- ▶ Alice îi trimite lui Bob mesajul  $(E(\mathbb{Z}_q), P, H_1)$ ;
- ▶ Bob alege  $y \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H_2 := yP$ ;
- ▶ Bob îi trimite  $H_2$  lui Alice și întoarce cheia  $k_B := yH_1$ ;
- ▶ Alice primește  $H_2$  și întoarce cheia  $k_A = xH_2$ .

# Schimbul de chei Diffie-Hellman pe curbe eliptice

- ▶ Corectitudinea protocolului presupune ca  $k_A = k_B$ , ceea ce se verifică ușor:
- ▶ Bob calculează cheia

$$k_B = yH_1 = y(xP) = (xy)P$$

- ▶ Alice calculează cheia

$$k_A = xH_2 = x(yP) = (xy)P$$

# Securitate

- ▶ O condiție **minimală** pentru ca protocolul să fie sigur este ca ECDLP să fie dificilă în  $\mathbb{G}$ ;

# Securitate

- ▶ O condiție **minimală** pentru ca protocolul să fie sigur este ca ECDLP să fie dificilă în  $\mathbb{G}$ ;
- ▶ **Întrebare:** Cum poate un adversar pasiv să determine cheia comună dacă poate sparge ECDLP?

# Securitate

- ▶ O condiție **minimală** pentru ca protocolul să fie sigur este ca ECDLP să fie dificilă în  $\mathbb{G}$ ;
- ▶ **Întrebare:** Cum poate un adversar pasiv să determine cheia comună dacă poate sparge ECDLP?
- ▶ **Răspuns:** Ascultă mediul de comunicație și preia mesajele  $H_1$  și  $H_2$ . Rezolvă *ECDLP* pentru  $H_1$  și determină  $x$ , apoi calculează  $k_A = k_B = xH_2$ .



- ▶ O condiție **minimală** pentru ca protocolul să fie sigur este ca ECDLP să fie dificilă în  $\mathbb{G}$ ;
- ▶ **Întrebare:** Cum poate un adversar pasiv să determine cheia comună dacă poate sparge ECDLP?
- ▶ **Răspuns:** Ascultă mediul de comunicație și preia mesajele  $H_1$  și  $H_2$ . Rezolvă *ECDLP* pentru  $H_1$  și determină  $x$ , apoi calculează  $k_A = k_B = xH_2$ .
- ▶ Aceasta nu este însă singura condiție necesară pentru a proteja protocolul de un atacator pasiv!

# ECCDH (Elliptic Curve Computational Diffie-Hellman)

- ▶ O condiție mai potrivită ar fi că adversarul să nu poată determina cheia comună  $k_A = k_B$ , chiar dacă are acces la întreaga comunicație;

# ECCDH (Elliptic Curve Computational Diffie-Hellman)

- ▶ O condiție mai potrivită ar fi că adversarul să nu poată determina cheia comună  $k_A = k_B$ , chiar dacă are acces la întreaga comunicație;
- ▶ Aceasta este **problema de calculabilitate Diffie-Hellman pe curbe eliptice (ECCDH)**: Fiind date curba eliptică  $E(\mathbb{Z}_q)$ , un punct  $P$  pe curbă și 2 alte puncte  $H_1, H_2 \xleftarrow{R} E(\mathbb{Z}_q)$ , să se determine:

$$ECCDH(H_1, H_2) = (ECDLP(P, H_1)ECDLP(P, H_2))P$$

# ECCDH (Elliptic Curve Computational Diffie-Hellman)

- ▶ O condiție mai potrivită ar fi că adversarul să nu poată determina cheia comună  $k_A = k_B$ , chiar dacă are acces la întreaga comunicație;
- ▶ Aceasta este **problema de calculabilitate Diffie-Hellman pe curbe eliptice (ECCDH)**: Fiind date curba eliptică  $E(\mathbb{Z}_q)$ , un punct  $P$  pe curbă și 2 alte puncte  $H_1, H_2 \xleftarrow{R} E(\mathbb{Z}_q)$ , să se determine:

$$ECCDH(H_1, H_2) = (ECDLP(P, H_1)ECDLP(P, H_2))P$$

- ▶ Pentru schimbul de chei Diffie-Hellman, rezolvarea ECDDH înseamnă că adversarul determină  $k_A = k_B = xyP$  cunoscând  $H_1, H_2, E(\mathbb{Z}_q), P$  (toate disponibile pe mediul de transmisiune nesecurizat).

# ECDDH (Elliptic Curve Decisional Diffie-Hellman)

- Nici această condiție nu este suficientă: chiar dacă adversarul nu poate determina cheia exactă, poate de exemplu să determine părți din ea;

# ECDDH (Elliptic Curve Decisional Diffie-Hellman)

- ▶ Nici această condiție nu este suficientă: chiar dacă adversarul nu poate determina cheia exactă, poate de exemplu să determine părți din ea;
- ▶ O condiție și mai potrivită este ca pentru adversar, cheia  $k_A = k_B$  să fie **indistinctibilă** față de o valoare aleatoare;

# ECDDH (Elliptic Curve Decisional Diffie-Hellman)

- ▶ Nici această condiție nu este suficientă: chiar dacă adversarul nu poate determina cheia exactă, poate de exemplu să determine părți din ea;
- ▶ O condiție și mai potrivită este ca pentru adversar, cheia  $k_A = k_B$  să fie **indistinctibilă** față de o valoare aleatoare;
- ▶ Sau, altfel spus, să satisfacă **problema de decidabilitate Diffie-Hellman pe curbe eliptice (ECDDH)**:

# ECDDH (Elliptic Curve Decisional Diffie-Hellman)

- ▶ Nici această condiție nu este suficientă: chiar dacă adversarul nu poate determina cheia exactă, poate de exemplu să determine părți din ea;
- ▶ O condiție și mai potrivită este ca pentru adversar, cheia  $k_A = k_B$  să fie **indistinctibilă** față de o valoare aleatoare;
- ▶ Sau, altfel spus, să satisfacă **problema de decidabilitate Diffie-Hellman pe curbe eliptice (ECDDH)**:

## Definiție

*Spunem că problema decizională Diffie-Hellman (ECDDH) este dificilă (relativ la curba eliptică  $E(\mathbb{Z}_q)$ ), dacă pentru orice algoritm PPT  $\mathcal{A}$  există o funcție neglijabilă  $\text{negl}$  așa încât:*

$$|\Pr[\mathcal{A}(E(\mathbb{Z}_q), P, xP, yP, zP) = 1] - \Pr[\mathcal{A}(E(\mathbb{Z}_q), P, xP, yP, xyP) = 1]| \leq \text{negl}(n), \text{ unde } x, y, z \xleftarrow{R} \mathbb{Z}_q$$



# Atacul Man-in-the-Middle

- ▶ Am analizat până acum securitatea față de atacatori pasivi;

# Atacul Man-in-the-Middle

- ▶ Am analizat până acum securitatea față de atacatori pasivi;
- ▶ Arătăm acum că schimbul de chei Diffie-Hellman este total nesigur pentru un adversar activ ...

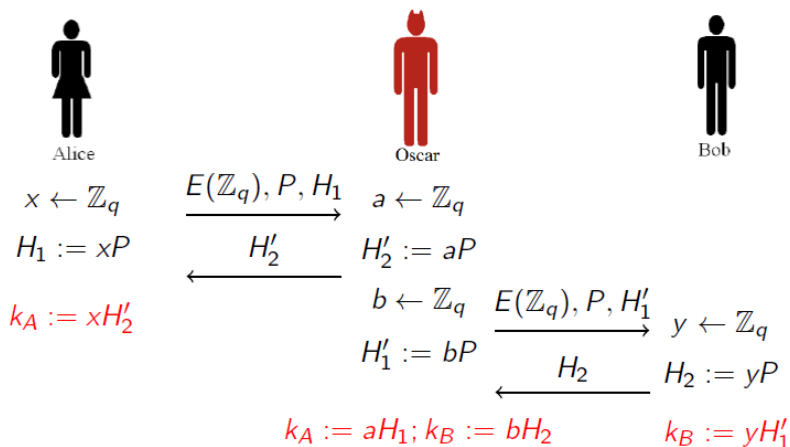
# Atacul Man-in-the-Middle

- ▶ Am analizat până acum securitatea față de atacatori pasivi;
- ▶ Arătăm acum că schimbul de chei Diffie-Hellman este total nesigur pentru un adversar activ ...
- ▶ ... care are dreptul de a intercepta, modifica, elimina mesajele de pe calea de comunicație;

# Atacul Man-in-the-Middle

- ▶ Am analizat până acum securitatea față de atacatori pasivi;
- ▶ Arătăm acum că schimbul de chei Diffie-Hellman este total nesigur pentru un adversar activ ...
- ▶ ... care are dreptul de a intercepta, modifica, elimina mesajele de pe calea de comunicație;
- ▶ Un astfel de adversar se poate interpune între Alice și Bob, dând naștere unui atac de tip **Man-in-the-Middle**.

# Atacul Man-in-the-Middle



# Atacul Man-in-the-Middle

- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$  și  $P$  un punct pe curbă;

# Atacul Man-in-the-Middle

- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$  și  $P$  un punct pe curbă;
- ▶ Alice alege  $x \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H_1 := xP$ ;

## Atacul Man-in-the-Middle

- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$  și  $P$  un punct pe curbă;
- ▶ Alice alege  $x \leftarrow^R \mathbb{Z}_q$  și calculează  $H_1 := xP$ ;
- ▶ Alice îi trimite lui Bob mesajul  $(E(\mathbb{Z}_q), P, H_1)$ ;



# Atacul Man-in-the-Middle

- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$  și  $P$  un punct pe curbă;
- ▶ Alice alege  $x \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H_1 := xP$ ;
- ▶ Alice îi trimite lui Bob mesajul  $(E(\mathbb{Z}_q), P, H_1)$ ;
- ▶ Oscar interceptează mesajul și răspunde lui Alice în locul lui Bob: alege  $a \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H'_2 := aP$ ;

# Atacul Man-in-the-Middle

- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$  și  $P$  un punct pe curbă;
- ▶ Alice alege  $x \leftarrow^R \mathbb{Z}_q$  și calculează  $H_1 := xP$ ;
- ▶ Alice îi trimite lui Bob mesajul  $(E(\mathbb{Z}_q), P, H_1)$ ;
- ▶ Oscar interceptează mesajul și răspunde lui Alice în locul lui Bob: alege  $a \leftarrow^R \mathbb{Z}_q$  și calculează  $H'_2 := aP$ ;
- ▶ Oscar și Alice dețin acum cheia comună  $k_A = axP$ ;

# Atacul Man-in-the-Middle

- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$  și  $P$  un punct pe curbă;
- ▶ Alice alege  $x \leftarrow^R \mathbb{Z}_q$  și calculează  $H_1 := xP$ ;
- ▶ Alice îi trimite lui Bob mesajul  $(E(\mathbb{Z}_q), P, H_1)$ ;
- ▶ Oscar interceptează mesajul și răspunde lui Alice în locul lui Bob: alege  $a \leftarrow^R \mathbb{Z}_q$  și calculează  $H'_2 := aP$ ;
- ▶ Oscar și Alice dețin acum cheia comună  $k_A = axP$ ;
- ▶ Oscar inițiază, în locul lui Alice, o nouă sesiune cu Bob: alege  $b \leftarrow^R \mathbb{Z}_q$  și calculează  $H'_1 := bP$ ;

# Atacul Man-in-the-Middle

- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$  și  $P$  un punct pe curbă;
- ▶ Alice alege  $x \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H_1 := xP$ ;
- ▶ Alice îi trimite lui Bob mesajul  $(E(\mathbb{Z}_q), P, H_1)$ ;
- ▶ Oscar interceptează mesajul și răspunde lui Alice în locul lui Bob: alege  $a \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H'_2 := aP$ ;
- ▶ Oscar și Alice dețin acum cheia comună  $k_A = axP$ ;
- ▶ Oscar inițiază, în locul lui Alice, o nouă sesiune cu Bob: alege  $b \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H'_1 := bP$ ;
- ▶ Bob alege  $y \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H_2 := yP$ ;

# Atacul Man-in-the-Middle

- ▶ Alice generează o curbă eliptică  $E(\mathbb{Z}_q)$  și  $P$  un punct pe curbă;
- ▶ Alice alege  $x \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H_1 := xP$ ;
- ▶ Alice îi trimite lui Bob mesajul  $(E(\mathbb{Z}_q), P, H_1)$ ;
- ▶ Oscar interceptează mesajul și răspunde lui Alice în locul lui Bob: alege  $a \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H'_2 := aP$ ;
- ▶ Oscar și Alice dețin acum cheia comună  $k_A = axP$ ;
- ▶ Oscar inițiază, în locul lui Alice, o nouă sesiune cu Bob: alege  $b \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H'_1 := bP$ ;
- ▶ Bob alege  $y \xleftarrow{R} \mathbb{Z}_q$  și calculează  $H_2 := yP$ ;
- ▶ Oscar și Bob dețin acum cheia comună  $k_B = ybP$ .

# Atacul Man-in-the-Middle

- ▶ Atacul este posibil pentru că poate **impersona** pe Alice și pe Bob;

# Atacul Man-in-the-Middle

- ▶ Atacul este posibil pentru că poate **impersona** pe Alice și pe Bob;
- ▶ De fiecare dată când Alice va transmite un mesaj criptat către Bob, Oscar îl interceptează și îl previne să ajungă la Bob;

# Atacul Man-in-the-Middle

- ▶ Atacul este posibil pentru că poate **impersona** pe Alice și pe Bob;
- ▶ De fiecare dată când Alice va transmite un mesaj criptat către Bob, Oscar îl interceptează și îl previne să ajungă la Bob;
- ▶ Oscar îl decriptează folosind  $k_A$ , apoi îl recriptează folosind  $k_B$  și îl transmite către Bob;



# Atacul Man-in-the-Middle

- ▶ Atacul este posibil pentru că poate **impersona** pe Alice și pe Bob;
- ▶ De fiecare dată când Alice va transmite un mesaj criptat către Bob, Oscar îl interceptează și îl previne să ajungă la Bob;
- ▶ Oscar îl decriptează folosind  $k_A$ , apoi îl recriptează folosind  $k_B$  și îl transmite către Bob;
- ▶ Alice și Bob comunică fără să fie conștienți de existența lui Oscar.

# Important de reținut!

- ▶ Modalitatea de trecere de la o construcție peste  $(\mathbb{Z}_q, \cdot)$  la  $(E(\mathbb{Z}_q), +)$
- ▶ Prezumții criptografice: ECCDH, ECDDH
- ▶ Schimbul de chei Diffie-Hellman pe curbe eliptice păstrează proprietățile schimbului de chei Diffie Hellman definit peste  $\mathbb{G}$  grup ciclic de ordin  $q$