

riptografie și Securitate

- Prelegerea 21.1 - Schimbul de chei Diffie-Hellman

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

1. Definiție
2. Schimbul de chei Diffie-Hellman
3. Securitate

Primitive cu cheie publică

- ▶ Am văzut că bazele criptografiei cu cheie publică au fost puse de Diffie și Hellman în 1976 ...

Primitive cu cheie publică

- ▶ Am văzut că bazele criptografiei cu cheie publică au fost puse de Diffie și Hellman în 1976 ...
- ▶ ... când au introdus 3 primitive cu cheie publică diferite:
 1. **sisteme de criptare cu cheie publică**
 2. **semnături digitale**
 3. **schimb de chei**

Primitive cu cheie publică

- ▶ Am văzut că bazele criptografiei cu cheie publică au fost puse de Diffie și Hellman în 1976 ...
- ▶ ... când au introdus 3 primitive cu cheie publică diferite:
 1. **sisteme de criptare cu cheie publică**
 2. **semnături digitale**
 3. **schimb de chei**
- ▶ Deși au introdus 3 concepte diferite, Diffie și Hellman au introdus o singură construcție, pentru schimbul de chei.

Schimb de chei

- ▶ **Sistemele de criptare cu cheie publică** le-am studiat și le vom mai studia în detaliu;

Schimb de chei

- ▶ **Sistemele de criptare cu cheie publică** le-am studiat și le vom mai studia în detaliu;
- ▶ **Semnăturile digitale** sunt analogul MAC-urilor din criptografia simetrică (sau corespondentul digital unei semnături reale);

Schimb de chei

- ▶ **Sistemele de criptare cu cheie publică** le-am studiat și le vom mai studia în detaliu;
- ▶ **Semnăturile digitale** sunt analogul MAC-urilor din criptografia simetrică (sau corespondentul digital unei semnături reale);
- ▶ **Schimbul de chei** îl introducem pentru a facilita introducerea sistemelor de criptare bazate pe DLP.

Schimb de chei

- Un **protocol de schimb de chei** este un protocol prin care 2 persoane care nu partajează în prealabil nici un secret pot genera o cheie comună, secretă;

Schimb de chei

- ▶ Un **protocol de schimb de chei** este un protocol prin care 2 persoane care nu partajează în prealabil nici un secret pot genera o cheie comună, secretă;
- ▶ Comunicarea necesară pentru stabilirea cheii se realizează printr-un canal public!

Schimb de chei

- ▶ Un **protocol de schimb de chei** este un protocol prin care 2 persoane care nu partajează în prealabil nici un secret pot genera o cheie comună, secretă;
- ▶ Comunicarea necesară pentru stabilirea cheii se realizează printr-un canal public!
- ▶ Deci un adversar poate intercepta toate mesajele transmise pe canalul de comunicație, dar NU trebuie să afle nimic despre cheia secretă obținută în urma protocolului;

Schimb de chei

- ▶ Un **protocol de schimb de chei** este un protocol prin care 2 persoane care nu partajează în prealabil nici un secret pot genera o cheie comună, secretă;
- ▶ Comunicarea necesară pentru stabilirea cheii se realizează printr-un canal public!
- ▶ Deci un adversar poate intercepta toate mesajele transmise pe canalul de comunicație, dar NU trebuie să afle nimic despre cheia secretă obținută în urma protocolului;
- ▶ Protocoalele de schimb de chei reprezintă o primitivă fundamentală în criptografie;

Schimb de chei

- ▶ Un **protocol de schimb de chei** este un protocol prin care 2 persoane care nu partajează în prealabil nici un secret pot genera o cheie comună, secretă;
- ▶ Comunicarea necesară pentru stabilirea cheii se realizează printr-un canal public!
- ▶ Deci un adversar poate intercepta toate mesajele transmise pe canalul de comunicație, dar NU trebuie să afle nimic despre cheia secretă obținută în urma protocolului;
- ▶ Protocoalele de schimb de chei reprezintă o primitivă fundamentală în criptografie;
- ▶ În continuare, ne vom rezuma strict la **schimbul de chei Diffie-Hellman**.

Schimbul de chei Diffie-Hellman



Alice

$$x \leftarrow \mathbb{Z}_q$$

$$h_1 := g^x$$

$$k_A := h_2^x$$



Bob

$$y \leftarrow \mathbb{Z}_q$$

$$h_2 := g^y$$

$$k_B := h_1^y$$

$$\mathbb{G}, q, g, h_1$$

$$h_2$$

Schimbul de chei Diffie-Hellman

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

Schimbul de chei Diffie-Hellman

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;
- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|q| = n$ și g un generator al grupului;

Schimbul de chei Diffie-Hellman

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;
- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|q| = n$ și g un generator al grupului;
- ▶ Alice alege $x \leftarrow^R \mathbb{Z}_q$ și calculează $h_1 := g^x$;

Schimbul de chei Diffie-Hellman

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;
- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|\mathbb{G}| = n$ și g un generator al grupului;
- ▶ Alice alege $x \leftarrow^R \mathbb{Z}_q$ și calculează $h_1 := g^x$;
- ▶ Alice îi trimite lui Bob mesajul (\mathbb{G}, g, q, h_1) ;

Schimbul de chei Diffie-Hellman

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;
- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|\mathbb{G}| = n$ și g un generator al grupului;
- ▶ Alice alege $x \leftarrow^R \mathbb{Z}_q$ și calculează $h_1 := g^x$;
- ▶ Alice îi trimite lui Bob mesajul (\mathbb{G}, g, q, h_1) ;
- ▶ Bob alege $y \leftarrow^R \mathbb{Z}_q$ și calculează $h_2 := g^y$;

Schimbul de chei Diffie-Hellman

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;
- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|\mathbb{G}| = n$ și g un generator al grupului;
- ▶ Alice alege $x \leftarrow^R \mathbb{Z}_q$ și calculează $h_1 := g^x$;
- ▶ Alice îi trimite lui Bob mesajul (\mathbb{G}, g, q, h_1) ;
- ▶ Bob alege $y \leftarrow^R \mathbb{Z}_q$ și calculează $h_2 := g^y$;
- ▶ Bob îi trimite h_2 lui Alice și întoarce cheia $k_B := h_1^y$;

Schimbul de chei Diffie-Hellman

- ▶ Alice și Bob doresc să stabilească o cheie secretă comună;
- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|\mathbb{G}| = n$ și g un generator al grupului;
- ▶ Alice alege $x \leftarrow^R \mathbb{Z}_q$ și calculează $h_1 := g^x$;
- ▶ Alice îi trimite lui Bob mesajul (\mathbb{G}, g, q, h_1) ;
- ▶ Bob alege $y \leftarrow^R \mathbb{Z}_q$ și calculează $h_2 := g^y$;
- ▶ Bob îi trimite h_2 lui Alice și întoarce cheia $k_B := h_1^y$;
- ▶ Alice primește h_2 și întoarce cheia $k_A = h_2^x$.

Schimbul de chei Diffie-Hellman

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

$$k_B = h_1^y = (g^x)^y = g^{xy}$$

- ▶ Alice calculează cheia

$$k_A = h_2^x = (g^y)^x = g^{xy}$$

Securitate

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

Securitate

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

Securitate

- ▶ O condiție **minimală** pentru ca protocolul să fie sigur este ca DLP să fie dificilă în \mathbb{G} ;
- ▶ **Întrebare:** Cum poate un adversar pasiv să determine cheia comună dacă poate sparge DLP?
- ▶ **Răspuns:** Ascultă mediul de comunicație și preia mesajele h_1 și h_2 . Rezolvă *DLP* pentru h_1 și determină x , apoi calculează $k_A = k_B = h_2^x$.

Securitate

- ▶ O condiție **minimală** pentru ca protocolul să fie sigur este ca DLP să fie dificilă în \mathbb{G} ;
- ▶ **Întrebare:** Cum poate un adversar pasiv să determine cheia comună dacă poate sparge DLP?
- ▶ **Răspuns:** Ascultă mediul de comunicație și preia mesajele h_1 și h_2 . Rezolvă *DLP* pentru h_1 și determină x , apoi calculează $k_A = k_B = h_2^x$.
- ▶ Aceasta nu este însă singura condiție necesară pentru a proteja protocolul de un atacator pasiv!

CDH (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;

CDH (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 (CDH)**: Fiind date grupul ciclic \mathbb{G} , un generator g al său și 2 elemente $h_1, h_2 \xleftarrow{R} \mathbb{G}$, să se determine:

$$CDH(h_1, h_2) = g^{\log_g h_1 \log_g h_2}$$

CDH (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 (CDH)**: Fiind date grupul ciclic \mathbb{G} , un generator g al său și 2 elemente $h_1, h_2 \xleftarrow{R} \mathbb{G}$, să se determine:

$$CDH(h_1, h_2) = g^{\log_g h_1 \log_g h_2}$$

- ▶ Pentru schimbul de chei Diffie-Hellman, rezolvarea CDH înseamnă că adversarul determină $k_A = k_B = g^{xy}$ cunoscând h_1, h_2, \mathbb{G}, g (toate disponibile pe mediul de transmisiune nesecurizat).

DDH (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;

DDH (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;

DDH (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 (DDH)**:

DDH (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 (DDH)**:

Definiție

Spunem că problema decizională Diffie-Hellman (DDH) este dificilă (relativ la \mathbb{G}), dacă pentru orice algoritm PPT \mathcal{A} există o funcție neglijabilă negl așa încât:

$$|\Pr[\mathcal{A}(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] - \Pr[\mathcal{A}(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1]| \leq \text{negl}(n),$$

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 ...

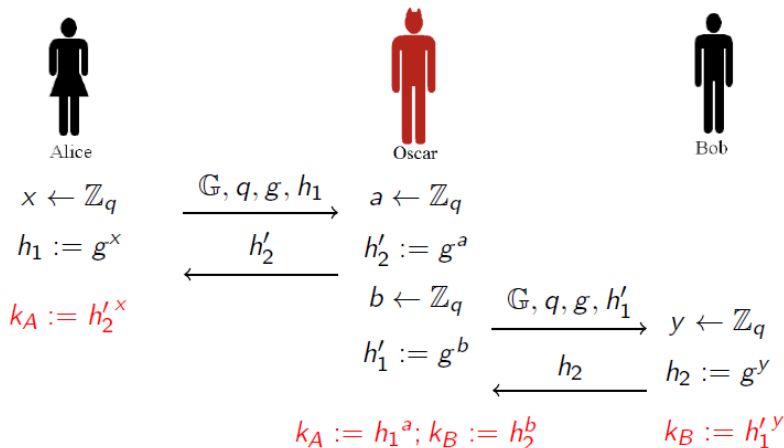
Atacul Man-in-the-Middle

- ▶ 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 un grup ciclic \mathbb{G} , de ordin q cu $|q| = n$ și g un generator al grupului;

Atacul Man-in-the-Middle

- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|\mathbb{G}| = n$ și g un generator al grupului;
- ▶ Alice alege $x \leftarrow^R \mathbb{Z}_q$ și calculează $h_1 := g^x$;

Atacul Man-in-the-Middle

- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|q| = n$ și g un generator al grupului;
- ▶ Alice alege $x \leftarrow^R \mathbb{Z}_q$ și calculează $h_1 := g^x$;
- ▶ Alice îi trimite lui Bob mesajul (\mathbb{G}, g, q, h_1) ;

Atacul Man-in-the-Middle

- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|\mathbb{G}| = n$ și g un generator al grupului;
- ▶ Alice alege $x \leftarrow^R \mathbb{Z}_q$ și calculează $h_1 := g^x$;
- ▶ Alice îi trimite lui Bob mesajul (\mathbb{G}, g, q, h_1) ;
- ▶ Oscar interceptează mesajul și răspunde lui Alice în locul lui Bob: alege $a \leftarrow^R \mathbb{Z}_q$ și calculează $h'_2 := g^a$;

Atacul Man-in-the-Middle

- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|q| = n$ și g un generator al grupului;
- ▶ Alice alege $x \leftarrow^R \mathbb{Z}_q$ și calculează $h_1 := g^x$;
- ▶ Alice îi trimite lui Bob mesajul (\mathbb{G}, g, q, h_1) ;
- ▶ Oscar interceptează mesajul și răspunde lui Alice în locul lui Bob: alege $a \leftarrow^R \mathbb{Z}_q$ și calculează $h'_2 := g^a$;
- ▶ Oscar și Alice dețin acum cheia comună $k_A = g^{xa}$;

Atacul Man-in-the-Middle

- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|q| = n$ și g un generator al grupului;
- ▶ Alice alege $x \leftarrow^R \mathbb{Z}_q$ și calculează $h_1 := g^x$;
- ▶ Alice îi trimite lui Bob mesajul (\mathbb{G}, g, q, h_1) ;
- ▶ Oscar interceptează mesajul și răspunde lui Alice în locul lui Bob: alege $a \leftarrow^R \mathbb{Z}_q$ și calculează $h'_2 := g^a$;
- ▶ Oscar și Alice dețin acum cheia comună $k_A = g^{xa}$;
- ▶ Oscar inițiază, în locul lui Alice, o nouă sesiune cu Bob: alege $b \leftarrow^R \mathbb{Z}_q$ și calculează $h'_1 := g^b$;

Atacul Man-in-the-Middle

- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|q| = n$ și g un generator al grupului;
- ▶ Alice alege $x \leftarrow^R \mathbb{Z}_q$ și calculează $h_1 := g^x$;
- ▶ Alice îi trimite lui Bob mesajul (\mathbb{G}, g, q, h_1) ;
- ▶ Oscar interceptează mesajul și răspunde lui Alice în locul lui Bob: alege $a \leftarrow^R \mathbb{Z}_q$ și calculează $h'_2 := g^a$;
- ▶ Oscar și Alice dețin acum cheia comună $k_A = g^{xa}$;
- ▶ Oscar inițiază, în locul lui Alice, o nouă sesiune cu Bob: alege $b \leftarrow^R \mathbb{Z}_q$ și calculează $h'_1 := g^b$;
- ▶ Bob alege $y \leftarrow^R \mathbb{Z}_q$ și calculează $h_2 := g^y$;

Atacul Man-in-the-Middle

- ▶ Alice generează un grup ciclic \mathbb{G} , de ordin q cu $|\mathbb{G}| = n$ și g un generator al grupului;
- ▶ Alice alege $x \xleftarrow{R} \mathbb{Z}_q$ și calculează $h_1 := g^x$;
- ▶ Alice îi trimite lui Bob mesajul (\mathbb{G}, g, q, h_1) ;
- ▶ Oscar interceptează mesajul și răspunde lui Alice în locul lui Bob: alege $a \xleftarrow{R} \mathbb{Z}_q$ și calculează $h'_2 := g^a$;
- ▶ Oscar și Alice dețin acum cheia comună $k_A = g^{xa}$;
- ▶ Oscar inițiază, în locul lui Alice, o nouă sesiune cu Bob: alege $b \xleftarrow{R} \mathbb{Z}_q$ și calculează $h'_1 := g^b$;
- ▶ Bob alege $y \xleftarrow{R} \mathbb{Z}_q$ și calculează $h_2 := g^y$;
- ▶ Oscar și Bob dețin acum cheia comună $k_B = g^{yb}$.

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!

- ▶ Schimbul de chei - o primitivă criptografică importantă
- ▶ Prezumții criptografice: CDH, DDH
- ▶ Schimbul de chei Diffie-Hellman nu rezistă la atacuri active