Kryptologia laboratorium 6-7.

Protokół Diffiego-Hellmana

Tomasz Gzella
Instytut Matematyki Stosowanej

WYDZIAŁ FIZYKI TECHNICZNEJ
I MATEMATYKI STOSOWANEJ

POLITECHNIKA
GDAŃSKA

Protokół Diffiego-Hellmana

Jest to protokół uzgadniania kluczy szyfrujących z 1976 r. Pozwala ustalić wspólny **tajny klucz** przy użyciu publicznych środków komunikacji. Opiera się głównie na arytmetyce multiplikatywnych grup modulo p (p - liczba pierwsza).
Przyjrzyjmy się przykładom, by zrozumieć działanie tego protokołu.
Dla ułatwienia informacje tajne będziemy oznaczać kolorem czerwonym.

Protokół Diffiego-Hellmana

Jest to protokół uzgadniania kluczy szyfrujących z 1976 r. Pozwala ustalić wspólny **tajny klucz** przy użyciu publicznych środków komunikacji. Opiera się głównie na arytmetyce multiplikatywnych grup modulo p (p - liczba pierwsza).
Przyjrzyjmy się przykładom, by zrozumieć działanie tego protokołu.
Dla ułatwienia informacje tajne będziemy oznaczać kolorem czerwonym.
Na początek wybierzmy $p = 7$
i przypomnijmy tabelę mnożenia w $\mathbb{Z}_7^*$:

Protokół Diffiego-Hellmana

Jest to protokół uzgadniania kluczy szyfrujących z 1976 r. Pozwala ustalić wspólny **tajny klucz** przy użyciu publicznych środków komunikacji. Opiera się głównie na arytmetyce multiplikatywnych grup modulo p (p - liczba pierwsza).
Przyjrzyjmy się przykładom, by zrozumieć działanie tego protokołu.
Dla ułatwienia informacje tajne będziemy oznaczać kolorem czerwonym.
Na początek wybierzmy $p = 7$
i przypomnijmy tabelę mnożenia w $\mathbb{Z}_7^*$:

$\cdot_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Algorytm opiera się na wielokrotnym potęgowaniu w pierścieniu $\mathbb{Z}_7^*$, zatem dla przykładu:

Algorytm opiera się na wielokrotnym potęgowaniu w pierścieniu $\mathbb{Z}_7^*$, zatem dla przykładu:

$$5^4(mod7) = 625(mod7) = 2$$

$$6^5(mod7) = 7776(mod7) = 6$$

$$6^6(mod7) = 46656(mod7) = 1$$

Algorytm opiera się na wielokrotnym potęgowaniu w pierścieniu $\mathbb{Z}_7^*$, zatem dla przykładu:

$$5^4(mod7) = 625(mod7) = 2$$

$$6^5(mod7) = 7776(mod7) = 6$$

$$6^6(mod7) = 46656(mod7) = 1$$

$$6^{6\cdot 6}(mod7) = 10\ 314\ 424\ 798\ 490\ 535\ 546\ 171\ 949\ 056(mod7) = 1$$

Algorytm opiera się na wielokrotnym potęgowaniu w pierścieniu $\mathbb{Z}_7^*$, zatem dla przykładu:

$$5^4(mod7) = 625(mod7) = 2$$

$$6^5(mod7) = 7776(mod7) = 6$$

$$6^6(mod7) = 46656(mod7) = 1$$

$$6^{6\cdot 6}(mod7) = 10\ 314\ 424\ 798\ 490\ 535\ 546\ 171\ 949\ 056(mod7) = 1$$

Lecz to tylko prosty przykład, a dla $\mathbb{Z}_{23}^*$ mamy już

Algorytm opiera się na wielokrotnym potęgowaniu w pierścieniu $\mathbb{Z}_7^*$, zatem dla przykładu:

$$5^4(mod7) = 625(mod7) = 2$$

$$6^5(mod7) = 7776(mod7) = 6$$

$$6^6(mod7) = 46656(mod7) = 1$$

$$6^{6\cdot 6}(mod7) = 10\ 314\ 424\ 798\ 490\ 535\ 546\ 171\ 949\ 056(mod7) = 1$$

Lecz to tylko prosty przykład, a dla $\mathbb{Z}_{23}^*$ mamy już
$5^{6\cdot 15} = 807793566946316088741610050849573099185363389551$
$639556884765625(mod23) = 2$
Z powyższych przykładów widać, że należy inaczej liczyć potęgi w pierścieniach modulo p.

Protokół Diffiego-Hellmana

Do użycia protokołu potrzebujemy liczb p, g oraz tajnych liczb, gdzie:

- p jest liczbą pierwszą,
- g jest generatorem grupy $\mathbb{Z}_p^*$,
- $a, b, \ldots \in \mathbb{Z}_p^*$ są tajnymi liczbami.

Protokół Diffiego-Hellmana

Do użycia protokołu potrzebujemy liczb p, g oraz tajnych liczb, gdzie:

- p jest liczbą pierwszą,
- g jest generatorem grupy $\mathbb{Z}_p^*$,
- $a, b, ... \in \mathbb{Z}_p^*$ są tajnymi liczbami.

Przypomnijmy zatem kilka faktów z algebry:

Twierdzenie (Małe twierdzenie Fermata)

Jeżeli p jest liczbą pierwszą i $p \nmid g$, *to*

$$g^{p-1} = 1 \ (mod \ p).$$

Protokół Diffiego-Hellmana

Do użycia protokołu potrzebujemy liczb p, g oraz tajnych liczb, gdzie:

- p jest liczbą pierwszą,
- g jest generatorem grupy $\mathbb{Z}_p^*$,
- $a, b, ... \in \mathbb{Z}_p^*$ są tajnymi liczbami.

Przypomnijmy zatem kilka faktów z algebry:

Twierdzenie (Małe twierdzenie Fermata)

Jeżeli p jest liczbą pierwszą i $p \nmid g$, *to*

$$g^{p-1} = 1 \ (mod \ p).$$

- jeśli p jest liczbą pierwszą, to $\mathbb{Z}_p^*$ jest grupą cykliczną,
- nie każdy element $g \in \mathbb{Z}_p^*$ jest generatorem tej grupy (rozważyć $1, 3, 10 \in \mathbb{Z}_{11}^*$)

Generatory grup - przykłady

- $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
  Generatory: $2, 6, 7, 8$

Generatory grup - przykłady

- $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
  Generatory: $2, 6, 7, 8$
  Nie są generatorami:
  $1^2 = 1$...

Generatory grup - przykłady

- $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
  Generatory: $2, 6, 7, 8$
  Nie są generatorami:
  $1^2 = 1 \ldots$
  $3^2 = 9, 3^3 = 9 \cdot 3 = 5, 3^4 = 5 \cdot 3 = 4, 3^5 = 4 \cdot 3 = 1$
  $10^2 = 1$

Generatory grup - przykłady

- $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
  Generatory: $2, 6, 7, 8$
  Nie są generatorami:
  $1^2 = 1 \ldots$
  $3^2 = 9, 3^3 = 9 \cdot 3 = 5, 3^4 = 5 \cdot 3 = 4, 3^5 = 4 \cdot 3 = 1$
  $10^2 = 1$

- $\mathbb{Z}_{17}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$
  Generatory: $3, 5, 6, 7, 10, 11, 12, 14$
  Nie są generatorami:
  $1^2 = 1 \ldots$
  $2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 15, 2^6 = 13, 2^7 = 9, 2^8 = 1$
  $16^2 = 1$

Generatory grup - przykłady

- $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
  Generatory: $2, 6, 7, 8$
  Nie są generatorami:
  $1^2 = 1 \ldots$
  $3^2 = 9, 3^3 = 9 \cdot 3 = 5, 3^4 = 5 \cdot 3 = 4, 3^5 = 4 \cdot 3 = 1$
  $10^2 = 1$

- $\mathbb{Z}_{17}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$
  Generatory: $3, 5, 6, 7, 10, 11, 12, 14$
  Nie są generatorami:
  $1^2 = 1 \ldots$
  $2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 15, 2^6 = 13, 2^7 = 9, 2^8 = 1$
  $16^2 = 1$

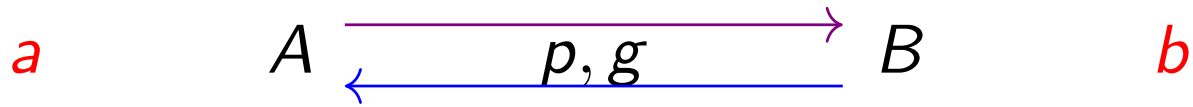
WNIOSKI: 1 oraz $p - 1$ nie są generatorami $\mathbb{Z}_p^*$.

Generatory grup - przykłady

- Generatory $\mathbb{Z}_{19}^* = \mathbb{Z}_{19} \setminus \{0\}$:
  $2, 3, 10, 13, 14, 15$
- Generatory $\mathbb{Z}_{23}^* = \mathbb{Z}_{23} \setminus \{0\}$:
  $5, 7, 10, 11, 14, 15, 17, 19, 20, 21$
- Generatory $\mathbb{Z}_{37}^* = \mathbb{Z}_{37} \setminus \{0\}$:
  $2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35$
- Generatory $\mathbb{Z}_{53}^* = \mathbb{Z}_{53} \setminus \{0\}$:
  $2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27,$
  $31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51$
- Generatory $\mathbb{Z}_{73}^* = \mathbb{Z}_{73} \setminus \{0\}$:
  $5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34,$
  $39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68$
- Generatory $\mathbb{Z}_{97}^* = \mathbb{Z}_{97} \setminus \{0\}$:
  $5, 7, 10, 13, 14, 15, 17, 21, 23, 26, 29, 37,$
  $38, 39, 40, 41, 56, 57, 58, 59, 60, 68, 71,$
  $74, 76, 80, 82, 83, 84, 87, 90, 92$

Protokół Diffiego-Hellmana dla 2 osób

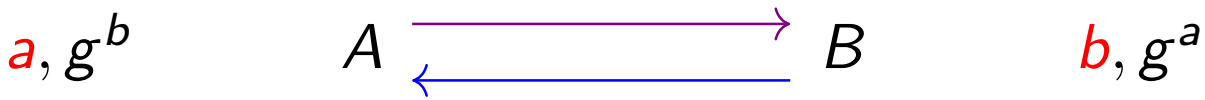
Alicja i Bob uzgodnili liczbę pierwszą p oraz generator g w $\mathbb{Z}_p^*$.
Każde z nich wybrało też swoją tajną liczbę: Alicja a, a Bob b.



Dane przekazane publicznie: p, g,

Protokół Diffiego-Hellmana dla 2 osób

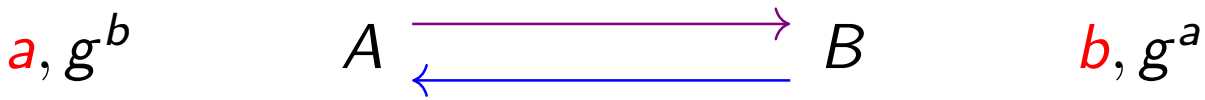
Alicja i Bob uzgodnili liczbę pierwszą p oraz generator g w $\mathbb{Z}_p^*$.
Każde z nich wybrało też swoją tajną liczbę: Alicja a, a Bob b.



Dane przekazane publicznie: p, g, g^a, g^b

Protokół Diffiego-Hellmana dla 2 osób

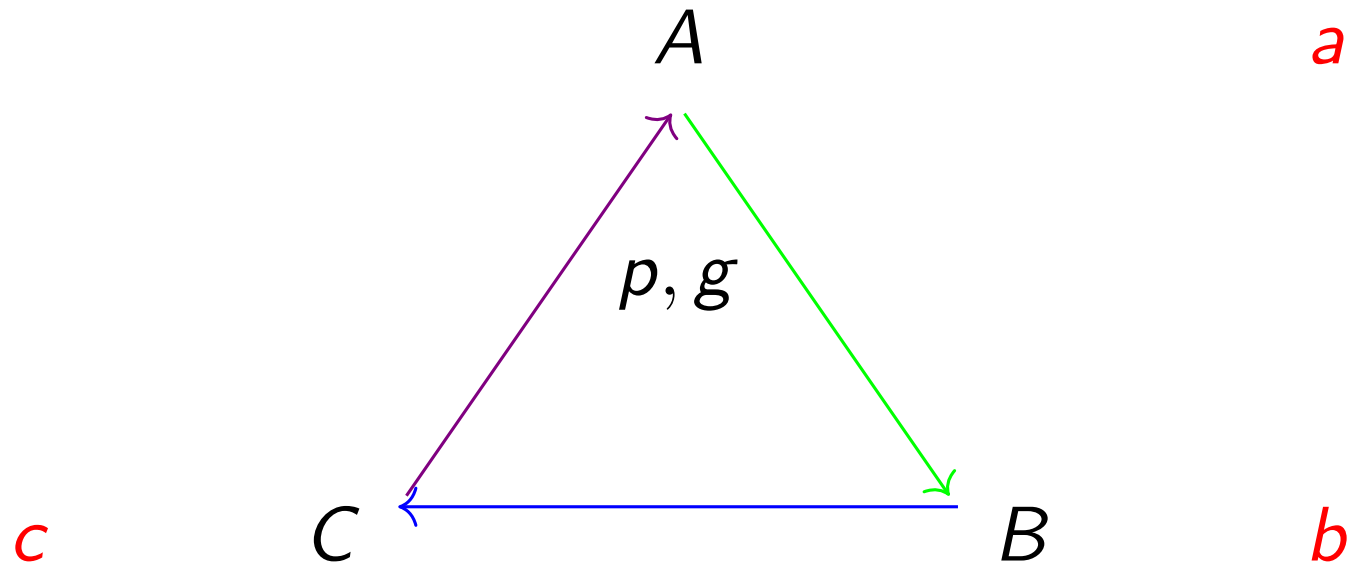
Alicja i Bob uzgodnili liczbę pierwszą p oraz generator g w $\mathbb{Z}_p^*$.
Każde z nich wybrało też swoją tajną liczbę: Alicja a, a Bob b.



Dane przekazane publicznie: p, g, g^a, g^b
Alicja wylicza $(g^b)^a$, Bob wylicza $(g^a)^b$
Uzgodniony wspólnie tajny klucz: $g^{ab} = (g^a)^b = (g^b)^a$

Protokół Diffiego-Hellmana dla 3 osób

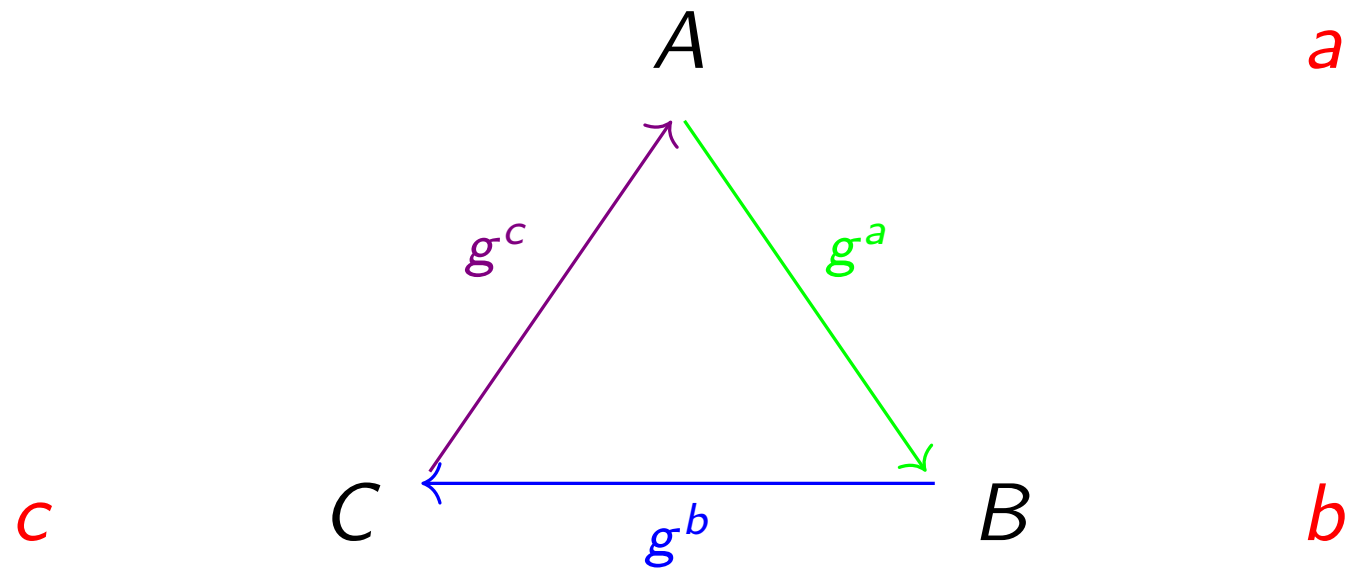
Alicja, Bob i Charlie uzgodnili liczbę pierwszą p oraz generator g w $\mathbb{Z}_p^*$. Każde z nich wybrało też swoją tajną liczbę: Alicja a, Bob b, a Charlie c.



Dane przekazane publicznie: p, g,

Protokół Diffiego-Hellmana dla 3 osób

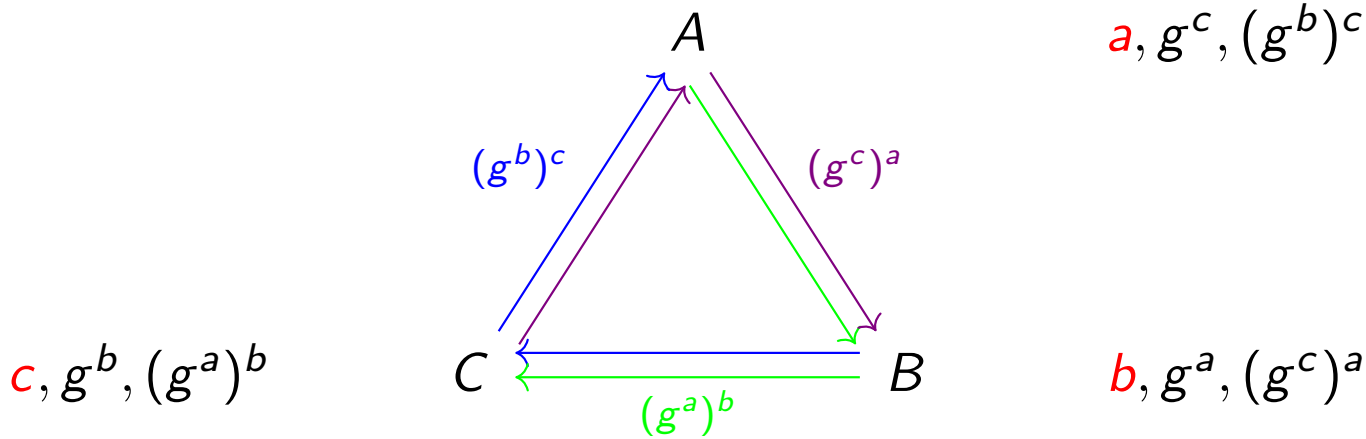
Alicja, Bob i Charlie uzgodnili liczbę pierwszą p oraz generator g w $\mathbb{Z}_p^*$. Każde z nich wybrało też swoją tajną liczbę: Alicja a, Bob b, a Charlie c.



Dane przekazane publicznie: $p, g, g^a, g^b, g^c,$

Protokół Diffiego-Hellmana dla 3 osób

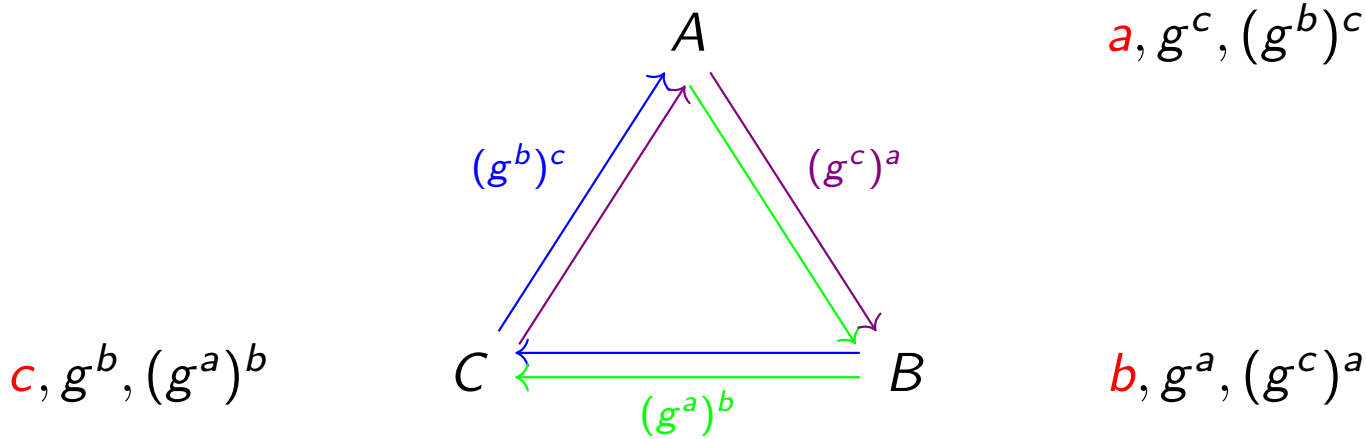
Alicja, Bob i Charlie uzgodnili liczbę pierwszą p oraz generator g w $\mathbb{Z}_p^*$. Każde z nich wybrało też swoją tajną liczbę: Alicja a, Bob b, a Charlie c.



Dane przekazane publicznie: $p, g, g^a, g^b, g^c, (g^c)^a, (g^a)^b, (g^b)^c$

Protokół Diffiego-Hellmana dla 3 osób

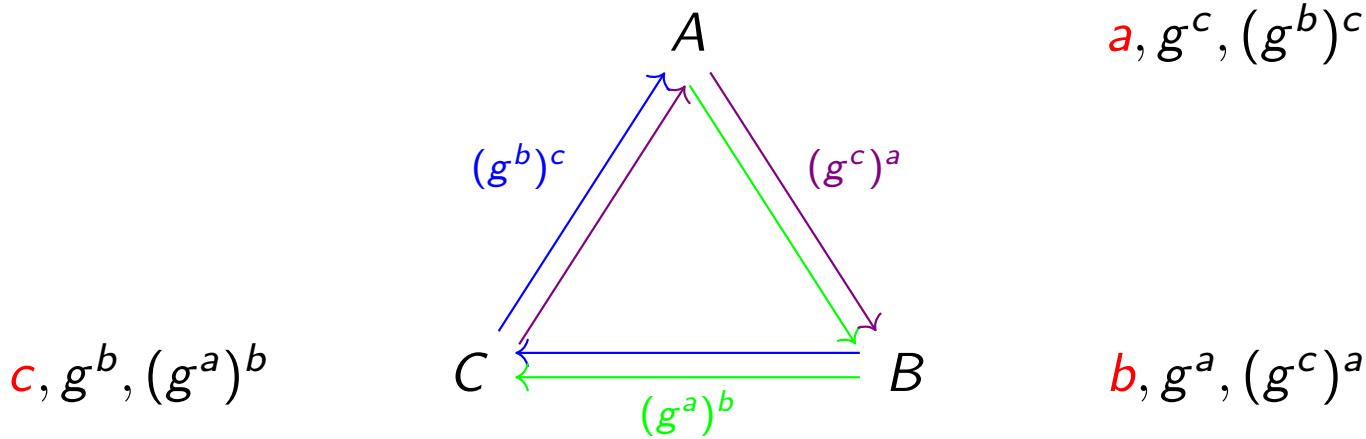
Alicja, Bob i Charlie uzgodnili liczbę pierwszą p oraz generator g w $\mathbb{Z}_p^*$. Każde z nich wybrało też swoją tajną liczbę: Alicja a, Bob b, a Charlie c.



Dane przekazane publicznie: $p, g, g^a, g^b, g^c, (g^c)^a, (g^a)^b, (g^b)^c$
Alicja wylicza $((g^b)^c)^a$, Bob wylicza $((g^c)^a)^b$, a Charlie $((g^a)^b)^c$
Uzgodniony wspólnie tajny klucz:
$g^{abc} = ((g^b)^c)^a = ((g^c)^a)^b = ((g^a)^b)^c$

Protokół Diffiego-Hellmana dla 3 osób

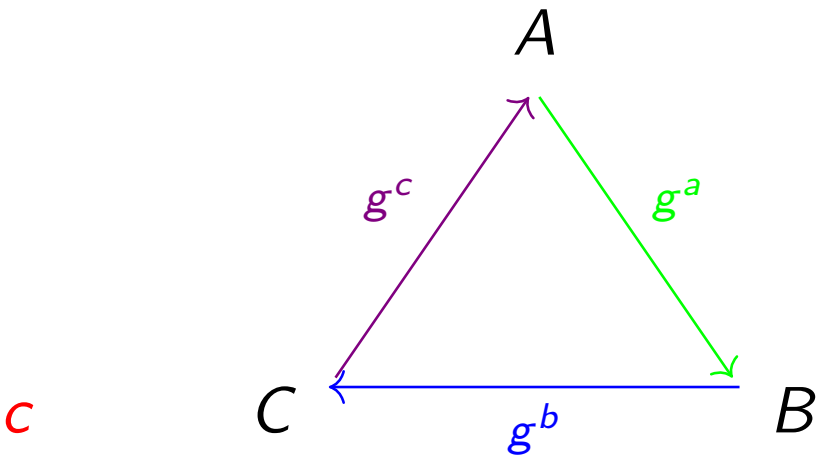
Alicja, Bob i Charlie uzgodnili liczbę pierwszą p oraz generator g w $\mathbb{Z}_p^*$. Każde z nich wybrało też swoją tajną liczbę: Alicja a, Bob b, a Charlie c.

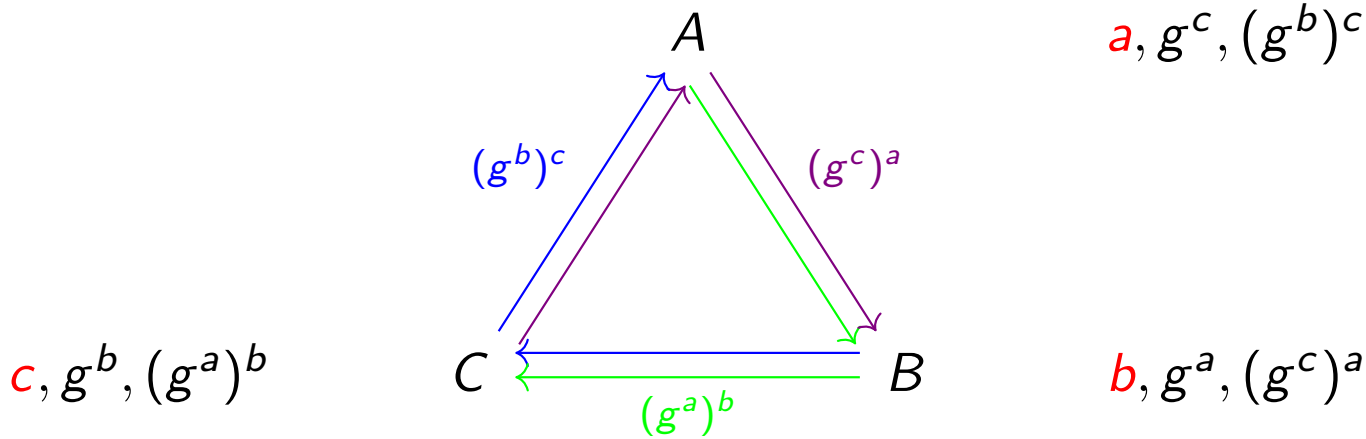


Dane przekazane publicznie: $p, g, g^a, g^b, g^c, (g^c)^a, (g^a)^b, (g^b)^c$
Alicja wylicza $((g^b)^c)^a$, Bob wylicza $((g^c)^a)^b$, a Charlie $((g^a)^b)^c$
Uzgodniony wspólnie tajny klucz:
$g^{abc} = ((g^b)^c)^a = ((g^c)^a)^b = ((g^a)^b)^c$
Ćwiczenie: Używając protokołu D-H uzgodnić tajny klucz (praca w grupach 2– lub 3–osobowych, bez programowania).

Protokół Diffiego-Hellmana - ćwiczenie

Ćwiczenie: Używając protokołu D-H uzgodnić tajny klucz (praca w grupach 2– lub 3–osobowych, bez programowania).





Metody ataku na protokół Diffiego-Hellmana

- **(atak brutalny)** Ewa zna p oraz g, więc może wyliczyć wszystkie potęgi g w $\mathbb{Z}_p^*$ i na podstawie przesyłanych informacji znaleźć a oraz b i ostatecznie g^{ab},
  - zamiast wyliczać po kolei, lepiej liczyć potęgi dla losowo wybranych wykładników z listy $\{1, ..., p-1\}$,

Metody ataku na protokół Diffiego-Hellmana

- **(atak brutalny)** Ewa zna p oraz g, więc może wyliczyć wszystkie potęgi g w $\mathbb{Z}_p^*$ i na podstawie przesyłanych informacji znaleźć a oraz b i ostatecznie g^{ab},
  - zamiast wyliczać po kolei, lepiej liczyć potęgi dla losowo wybranych wykładników z listy $\{1, ..., p-1\}$,
- **(metoda Shanksa, czyli małych i dużych kroków)** dane są elementy g, $h = g^a$ oraz $p = |G|$:
  - obliczamy $[\sqrt{p}] - 1$,
  - tworzymy listę $\{1, g, g^2, ..., g^{[\sqrt{p}]-1}\}$,
  - obliczamy $hg^{-i[\sqrt{p}]}$ dla kolejnych $i = 1, 2, ...$ i sprawdzamy, czy jest na liście,
  - jeśli element jest na liście, to znamy i oraz j (indeks elementu z listy), zachodzi więc równość

$$hg^{-i[\sqrt{p}]} = g^j \quad \Rightarrow \quad h = g^{i[\sqrt{p}]+j}.$$

Metoda Shanksa - przykład

Dane są elementy $g = 5$, $h = g^5 = 14$ oraz $p = 17 = |\mathbb{Z}_{17}|$:

Metoda Shanksa - przykład

Dane są elementy $g = 5$, $h = g^5 = 14$ oraz $p = 17 = |\mathbb{Z}_{17}|$:

- obliczamy $[\sqrt{p}] - 1 = 4 - 1 = 3$,

Metoda Shanksa - przykład

Dane są elementy $g = 5$, $h = g^{5} = 14$ oraz $p = 17 = |\mathbb{Z}_{17}|$:

- obliczamy $[\sqrt{p}] - 1 = 4 - 1 = 3$,
- tworzymy listę $\{1, g, g^2, ..., g^{[\sqrt{p}]-1}\}$:

Metoda Shanksa - przykład

Dane są elementy $g = 5$, $h = g^5 = 14$ oraz $p = 17 = |\mathbb{Z}_{17}|$:

- obliczamy $[\sqrt{p}] - 1 = 4 - 1 = 3$,
- tworzymy listę $\{1, g, g^2, ..., g^{[\sqrt{p}]-1}\}$:

$$\{5^0, 5^1, 5^2, 5^3\} = \{1, 5, 8, 6\}.$$

Metoda Shanksa - przykład

Dane są elementy $g = 5$, $h = g^5 = 14$ oraz $p = 17 = |\mathbb{Z}_{17}|$:

- obliczamy $[\sqrt{p}] - 1 = 4 - 1 = 3$,
- tworzymy listę $\{1, g, g^2, ..., g^{[\sqrt{p}]-1}\}$:

$$\{5^0, 5^1, 5^2, 5^3\} = \{1, 5, 8, 6\}.$$

- obliczamy $hg^{-i[\sqrt{p}]}$ dla kolejnych $i = 1, 2, ...$ i sprawdzamy, czy jest na liście,

Metoda Shanksa - przykład

Dane są elementy $g = 5$, $h = g^5 = 14$ oraz $p = 17 = |\mathbb{Z}_{17}|$:

- obliczamy $[\sqrt{p}] - 1 = 4 - 1 = 3$,
- tworzymy listę $\{1, g, g^2, ..., g^{[\sqrt{p}]-1}\}$:

$$\{5^0, 5^1, 5^2, 5^3\} = \{1, 5, 8, 6\}.$$

- obliczamy $hg^{-i[\sqrt{p}]}$ dla kolejnych $i = 1, 2, ...$ i sprawdzamy, czy jest na liście,
  Zauważmy, że $5^{-1} = 7$.

Metoda Shanksa - przykład

Dane są elementy $g = 5$, $h = g^5 = 14$ oraz $p = 17 = |\mathbb{Z}_{17}|$:

- obliczamy $[\sqrt{p}] - 1 = 4 - 1 = 3$,
- tworzymy listę $\{1, g, g^2, ..., g^{[\sqrt{p}]-1}\}$:

$$\{5^0, 5^1, 5^2, 5^3\} = \{1, 5, 8, 6\}.$$

- obliczamy $hg^{-i[\sqrt{p}]}$ dla kolejnych $i = 1, 2, ...$ i sprawdzamy, czy jest na liście,
  Zauważmy, że $5^{-1} = 7$.

$$hg^{-1 \cdot 4} = 14 \cdot 5^{-4} =$$

Metoda Shanksa - przykład

Dane są elementy $g = 5$, $h = g^5 = 14$ oraz $p = 17 = |\mathbb{Z}_{17}|$:

- obliczamy $[\sqrt{p}] - 1 = 4 - 1 = 3$,
- tworzymy listę $\{1, g, g^2, ..., g^{[\sqrt{p}]-1}\}$:

$$\{5^0, 5^1, 5^2, 5^3\} = \{1, 5, 8, 6\}.$$

- obliczamy $hg^{-i[\sqrt{p}]}$ dla kolejnych $i = 1, 2, ...$ i sprawdzamy, czy jest na liście,
  Zauważmy, że $5^{-1} = 7$.

$$hg^{-1\cdot 4} = 14 \cdot 5^{-4} = 14 \cdot 7^4 = 5 \text{ (STOP)}$$

Metoda Shanksa - przykład

Dane są elementy $g = 5$, $h = g^5 = 14$ oraz $p = 17 = |\mathbb{Z}_{17}|$:

- obliczamy $[\sqrt{p}] - 1 = 4 - 1 = 3$,
- tworzymy listę $\{1, g, g^2, ..., g^{[\sqrt{p}]-1}\}$:

$$\{5^0, 5^1, 5^2, 5^3\} = \{1, 5, 8, 6\}.$$

- obliczamy $hg^{-i[\sqrt{p}]}$ dla kolejnych $i = 1, 2, ...$ i sprawdzamy, czy jest na liście,
  Zauważmy, że $5^{-1} = 7$.

$$hg^{-1\cdot 4} = 14 \cdot 5^{-4} = 14 \cdot 7^4 = 5 \text{ (STOP)}$$

$$hg^{-2\cdot 4} = ..., \quad hg^{-3\cdot 4} = ..., \text{ (tego już nie liczymy)}$$

Metoda Shanksa - przykład

Dane są elementy $g = 5$, $h = g^5 = 14$ oraz $p = 17 = |\mathbb{Z}_{17}|$:

- obliczamy $[\sqrt{p}] - 1 = 4 - 1 = 3$,
- tworzymy listę $\{1, g, g^2, ..., g^{[\sqrt{p}]-1}\}$:

$$\{5^0, 5^1, 5^2, 5^3\} = \{1, 5, 8, 6\}.$$

- obliczamy $hg^{-i[\sqrt{p}]}$ dla kolejnych $i = 1, 2, ...$ i sprawdzamy, czy jest na liście,
  Zauważmy, że $5^{-1} = 7$.

$$hg^{-1\cdot 4} = 14 \cdot 5^{-4} = 14 \cdot 7^4 = 5 \text{ (STOP)}$$

$$hg^{-2\cdot 4} = ..., \quad hg^{-3\cdot 4} = ..., \text{ (tego już nie liczymy)}$$

- jeśli element jest na liście (a $5 = 5^1$ jest na liście),

Metoda Shanksa - przykład

Dane są elementy $g = 5$, $h = g^5 = 14$ oraz $p = 17 = |\mathbb{Z}_{17}|$:

- obliczamy $[\sqrt{p}] - 1 = 4 - 1 = 3$,
- tworzymy listę $\{1, g, g^2, ..., g^{[\sqrt{p}]-1}\}$:

$$\{5^0, 5^1, 5^2, 5^3\} = \{1, 5, 8, 6\}.$$

- obliczamy $hg^{-i[\sqrt{p}]}$ dla kolejnych $i = 1, 2, ...$ i sprawdzamy, czy jest na liście,
  Zauważmy, że $5^{-1} = 7$.

$$hg^{-1\cdot 4} = 14 \cdot 5^{-4} = 14 \cdot 7^4 = 5 \text{ (STOP)}$$

$$hg^{-2\cdot 4} = ..., \quad hg^{-3\cdot 4} = ..., \text{ (tego już nie liczymy)}$$

- jeśli element jest na liście (a $5 = 5^1$ jest na liście), to znamy $i = 1$ oraz $j = 1$, zachodzi więc równość

$$h = g^{i[\sqrt{p}]+j} = g^{4+1} = g^5.$$

Algorytm Euklidesa - przykłady

Do obliczenia $5^{-1} = 7$ w $\mathbb{Z}_{17}$ użyliśmy algorytmu Euklidesa:

Algorytm Euklidesa - przykłady

Do obliczenia $5^{-1} = 7$ w $\mathbb{Z}_{17}$ użyliśmy algorytmu Euklidesa:

17	1	0	

Algorytm Euklidesa - przykłady

Do obliczenia $5^{-1} = 7$ w $\mathbb{Z}_{17}$ użyliśmy algorytmu Euklidesa:

17	1	0	
5	0	1	

Algorytm Euklidesa - przykłady

Do obliczenia $5^{-1} = 7$ w $\mathbb{Z}_{17}$ użyliśmy algorytmu Euklidesa:

17	1	0	
5	0	1	(-3)

Algorytm Euklidesa - przykłady

Do obliczenia $5^{-1} = 7$ w $\mathbb{Z}_{17}$ użyliśmy algorytmu Euklidesa:

17	1	0	
5	0	1	(-3)
2	1	-3	

Algorytm Euklidesa - przykłady

Do obliczenia $5^{-1} = 7$ w $\mathbb{Z}_{17}$ użyliśmy algorytmu Euklidesa:

17	1	0	
5	0	1	(-3)
2	1	-3	(-2)

Algorytm Euklidesa - przykłady

Do obliczenia $5^{-1} = 7$ w $\mathbb{Z}_{17}$ użyliśmy algorytmu Euklidesa:

17	1	0	
5	0	1	(-3)
2	1	-3	(-2)
1	-2	7	*STOP*

Algorytm Euklidesa - przykłady

Do obliczenia $5^{-1} = 7$ w $\mathbb{Z}_{17}$ użyliśmy algorytmu Euklidesa:

17	1	0	
5	0	1	(-3)
2	1	-3	(-2)
1	-2	7	*STOP*

Stąd

$$1 = -2 \cdot 17 + 7 \cdot 5,$$

czyli

$$5 \cdot 7 = 1 \pmod{17},$$

zatem

$$5^{-1} = 7 \pmod{17}.$$