Teori Bilangan Elementer Bagian 3 (Suplemen)

CRT dan DHKE (Suplemen)

MZI

Fakultas Informatika
Telkom University

FIF Tel-U

Juni 2023

Acknowledgements

Slide ini disusun berdasarkan materi yang terdapat pada sumber-sumber berikut:

1. *Discrete Mathematics and Its Applications*, Edisi 8, 2019, oleh K. H. Rosen (acuan utama).
2. *Discrete Mathematics with Applications*, Edisi 5, 2018, oleh S. S. Epp.
3. *Mathematics for Computer Science*. MIT, 2010, oleh E. Lehman, F. T. Leighton, A. R. Meyer.
4. *Slide* kuliah Matematika Diskret 2 (2012) di Fasilkom UI oleh B. H. Widjaja.
5. Slide kuliah Matematika Diskret 1 di Fasilkom UI oleh A. A. Krisnadhi.
6. *Slide* kuliah Matematika Diskrit di Telkom University oleh B. Purnama.

Beberapa gambar dapat diambil dari sumber-sumber di atas. *Slide* ini ditujukan untuk keperluan akademis di lingkungan FIF Telkom University. Jika Anda memiliki saran/ pendapat/ pertanyaan terkait materi dalam *slide* ini, silakan kirim email ke `<pleasedontspam>@telkomuniversity.ac.id`.

Bahasan

1. Teorema Sisa Tiongkok (Chinese Remainder Theorem)

2. Protokol Diffie-Hellman (Diffie-Hellman Key Exchange)

Bahasan

Motivasi: Menghitung dari Sisa Pembagian

Perhatikan cerita berikut.

Permasalahan

Seorang kakek penjual buah mangga ingin menghitung berapa banyak buah mangganya yang tersisa di gudang. Kakek tersebut tidak mengetahui persis berapa banyak buah mangga yang tersisa, namun ia hanya mengetahui bahwa:

1. jika banyak buah mangga dibagi 3, maka sisanya 2;
2. jika banyak buah mangga dibagi 5, maka sisanya 3;
3. banyaknya buah mangga di gudang adalah antara 100 sampai 120 buah.

Dapatkah Anda menentukan berapa banyak sisa buah mangga yang ada di gudang secara pasti?

Model Matematika Permasalahan

Misalkan banyaknya buah mangga adalah x, maka kita memiliki model matematika berikut:

1. jika banyak buah mangga dibagi 3, maka sisanya 2;

Model Matematika Permasalahan

Misalkan banyaknya buah mangga adalah x, maka kita memiliki model matematika berikut:

1. jika banyak buah mangga dibagi 3, maka sisanya 2;
   artinya jika x dibagi 3, maka sisanya 2; sehingga diperoleh $x \bmod 3 = 2$, atau $x \equiv 2 \pmod 3$;
2. jika banyak buah mangga dibagi 5, maka sisanya 3

Model Matematika Permasalahan

Misalkan banyaknya buah mangga adalah x, maka kita memiliki model matematika berikut:

1. jika banyak buah mangga dibagi 3, maka sisanya 2;
   artinya jika x dibagi 3, maka sisanya 2; sehingga diperoleh $x \bmod 3 = 2$, atau $x \equiv 2 \pmod 3$;
2. jika banyak buah mangga dibagi 5, maka sisanya 3
   artinya jika x dibagi 5, maka sisanya 3; sehingga diperoleh $x \bmod 5 = 3$, atau $x \equiv 3 \pmod 5$;

Model Matematika Permasalahan

Misalkan banyaknya buah mangga adalah x, maka kita memiliki model matematika berikut:

1. jika banyak buah mangga dibagi 3, maka sisanya 2;
   artinya jika x dibagi 3, maka sisanya 2; sehingga diperoleh $x \bmod 3 = 2$, atau $x \equiv 2 \pmod 3$;
2. jika banyak buah mangga dibagi 5, maka sisanya 3
   artinya jika x dibagi 5, maka sisanya 3; sehingga diperoleh $x \bmod 5 = 3$, atau $x \equiv 3 \pmod 5$;
3. banyaknya buah mangga di gudang adalah antara 100 sampai 120 buah, atau $100 \leq x \leq 120$.

Akibatnya kita harus mencari x yang memenuhi semua sifat berikut:

$$x \equiv 2 \pmod 3 \quad (1)$$
$$x \equiv 3 \pmod 5 \quad (2)$$

dengan $100 \leq x \leq 120$. Dua kongruensi linier (1) dan (2) membentuk suatu sistem kongruensi linier.

Pencarian Solusi Sistem Kongruensi Linier

Dari (1) kita memiliki

$$x \equiv 2 \pmod 3 \text{, maka } x = 3s + 2, \text{ untuk } s \in \mathbb{Z},$$

dengan mensubstitusikan nilai ini ke (2), yaitu $x \equiv 3 \pmod 5$, kita memperoleh

Pencarian Solusi Sistem Kongruensi Linier

Dari (1) kita memiliki

$$x \equiv 2 \pmod 3 \text{, maka } x = 3s + 2 \text{, untuk } s \in \mathbb{Z},$$

dengan mensubstitusikan nilai ini ke (2), yaitu $x \equiv 3 \pmod 5$, kita memperoleh

$$3s + 2 \equiv 3 \pmod 5$$

Pencarian Solusi Sistem Kongruensi Linier

Dari (1) kita memiliki

$$x \equiv 2 \pmod 3 \text{, maka } x = 3s + 2 \text{, untuk } s \in \mathbb{Z},$$

dengan mensubstitusikan nilai ini ke (2), yaitu $x \equiv 3 \pmod 5$, kita memperoleh

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \end{aligned}$$

Pencarian Solusi Sistem Kongruensi Linier

Dari (1) kita memiliki

$$x \equiv 2 \pmod 3 \text{, maka } x = 3s + 2 \text{, untuk } s \in \mathbb{Z},$$

dengan mensubstitusikan nilai ini ke (2), yaitu $x \equiv 3 \pmod 5$, kita memperoleh

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5, \end{aligned}$$

sehingga diperoleh $s = 5t + 2$ untuk $t \in \mathbb{Z}$. Dengan mensubstitusikan nilai ini ke x, diperoleh

$$x =$$

Pencarian Solusi Sistem Kongruensi Linier

Dari (1) kita memiliki

$$x \equiv 2 \pmod 3 \text{, maka } x = 3s + 2 \text{, untuk } s \in \mathbb{Z},$$

dengan mensubstitusikan nilai ini ke (2), yaitu $x \equiv 3 \pmod 5$, kita memperoleh

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5, \end{aligned}$$

sehingga diperoleh $s = 5t + 2$ untuk $t \in \mathbb{Z}$. Dengan mensubstitusikan nilai ini ke x, diperoleh

$$x = 3s + 2 =$$

Pencarian Solusi Sistem Kongruensi Linier

Dari (1) kita memiliki

$$x \equiv 2 \pmod 3 \text{, maka } x = 3s + 2, \text{ untuk } s \in \mathbb{Z},$$

dengan mensubstitusikan nilai ini ke (2), yaitu $x \equiv 3 \pmod 5$, kita memperoleh

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5, \end{aligned}$$

sehingga diperoleh $s = 5t + 2$ untuk $t \in \mathbb{Z}$. Dengan mensubstitusikan nilai ini ke x, diperoleh

$$x = 3s + 2 = 3(5t + 2) + 2 = 15t + 8,$$

atau solusi yang dicari berbentuk $x \equiv 8 \pmod{15}$. Tinjau bahwa $8 \equiv 2 \pmod 3$ dan $8 \equiv 3 \pmod 5$. Kemudian, karena $105 \equiv 0 \pmod{15}$, maka kita dapat memilih $x =$

Pencarian Solusi Sistem Kongruensi Linier

Dari (1) kita memiliki

$$x \equiv 2 \pmod 3 \text{, maka } x = 3s + 2, \text{ untuk } s \in \mathbb{Z},$$

dengan mensubstitusikan nilai ini ke (2), yaitu $x \equiv 3 \pmod 5$, kita memperoleh

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5, \end{aligned}$$

sehingga diperoleh $s = 5t + 2$ untuk $t \in \mathbb{Z}$. Dengan mensubstitusikan nilai ini ke x, diperoleh

$$x = 3s + 2 = 3(5t + 2) + 2 = 15t + 8,$$

atau solusi yang dicari berbentuk $x \equiv 8 \pmod{15}$. Tinjau bahwa $8 \equiv 2 \pmod 3$ dan $8 \equiv 3 \pmod 5$. Kemudian, karena $105 \equiv 0 \pmod{15}$, maka kita dapat memilih $x = 105 + 8 = 113 \equiv 8 \pmod{15}$.

Kongruensi Linier Tiga Persamaan

Masalah penyelesaian kongruensi linier tiga persamaan sudah dijelaskan sejak zaman Tiongkok Kuno, tepatnya pada abad ke-1 M oleh Sun-Tsu. Pada *slide* ini kita akan membahas cara menyelesaikan kongruensi linier tiga persamaan atau lebih.

Gambar dari img5.epochtimes.com/i6/80118052019197 4.jpg.

Prajurit Jendral Xin Han

Permasalahan

Jenderal Xin Han memimpin sebuah pasukan yang terdiri atas 1500 prajurit. Dalam pertempuran, antara $400 - 500$ prajuritnya tewas. Untuk mengetahui secara pasti banyaknya prajurit yang tewas ia memerintahkan prajuritnya untuk melakukan instruksi berikut:

1. bentuk kelompok yang terdiri atas 3 prajurit; ternyata ada 2 prajurit yang tidak mendapat kelompok;
2. bentuk kelompok yang terdiri atas 5 prajurit; ternyata ada 3 prajurit yang tidak mendapat kelompok;
3. bentuk kelompok yang terdiri atas 7 prajurit; ternyata ada 2 prajurit yang tidak mendapat kelompok.

Melalui informasi di atas, tentukan secara pasti banyaknya prajurit yang tersisa.

Model Matematika

Dari permasalahan yang ada, kita dapat memperoleh sistem kongruensi linier berikut

$$x \equiv 2 \pmod 3 \tag{3}$$
$$x \equiv 3 \pmod 5 \tag{4}$$
$$x \equiv 2 \pmod 7, \tag{5}$$

x yang dicari haruslah memenuhi $1000 \leq x \leq 1100$.

Mencari x

Bilangan bulat x yang secara simultan memenuhi (3), (4), dan (5) dapat dicari menggunakan metode "substitusi balik" (*back substitution*) dengan langkah-langkah berikut:

Mencari x

Bilangan bulat x yang secara simultan memenuhi (3), (4), dan (5) dapat dicari menggunakan metode "substitusi balik" (*back substitution*) dengan langkah-langkah berikut:

- Dari kongruensi (3), diperoleh $3 \mid (x-2)$, sehingga $x = 3s + 2$, untuk $s \in \mathbb{Z}$.

Mencari x

Bilangan bulat x yang secara simultan memenuhi (3), (4), dan (5) dapat dicari menggunakan metode "substitusi balik" (*back substitution*) dengan langkah-langkah berikut:

- Dari kongruensi (3), diperoleh $3 \mid (x-2)$, sehingga $x = 3s + 2$, untuk $s \in \mathbb{Z}$.
- Dengan mensubstitusikan nilai $x = 3s + 2$ ke kongruensi (4) diperoleh

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5 \text{ (karena } 3^{-1} \equiv 2 \pmod 5 \text{).} \end{aligned}$$

Mencari x

Bilangan bulat x yang secara simultan memenuhi (3), (4), dan (5) dapat dicari menggunakan metode "substitusi balik" (*back substitution*) dengan langkah-langkah berikut:

- Dari kongruensi (3), diperoleh $3 | (x-2)$, sehingga $x = 3s + 2$, untuk $s \in \mathbb{Z}$.
- Dengan mensubstitusikan nilai $x = 3s + 2$ ke kongruensi (4) diperoleh

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5 \text{ (karena } 3^{-1} \equiv 2 \pmod 5 \text{)}. \end{aligned}$$

- Jadi diperoleh $5 | (s-2)$ atau $s = 5t + 2$, untuk $t \in \mathbb{Z}$.

Mencari x

Bilangan bulat x yang secara simultan memenuhi (3), (4), dan (5) dapat dicari menggunakan metode "substitusi balik" (*back substitution*) dengan langkah-langkah berikut:

- Dari kongruensi (3), diperoleh $3 \mid (x-2)$, sehingga $x = 3s + 2$, untuk $s \in \mathbb{Z}$.
- Dengan mensubstitusikan nilai $x = 3s + 2$ ke kongruensi (4) diperoleh

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5 \text{ (karena } 3^{-1} \equiv 2 \pmod 5 \text{).} \end{aligned}$$

- Jadi diperoleh $5 \mid (s-2)$ atau $s = 5t + 2$, untuk $t \in \mathbb{Z}$.
- Oleh karena itu diperoleh $x = 3s + 2 = 3(5t+2) + 2 = 15t + 8$. Dengan mensubstitusikan nilai $x = 15t + 8$ ke kongruensi (5) diperoleh

$$\begin{aligned} 15t + 8 &\equiv 2 \pmod 7 \text{, karena } 15t + 8 \equiv t + 1 \pmod 7 \text{, maka} \\ t + 1 &\equiv 2 \pmod 7 \\ t &\equiv 1 \pmod 7 . \end{aligned}$$

Mencari x

Bilangan bulat x yang secara simultan memenuhi (3), (4), dan (5) dapat dicari menggunakan metode "substitusi balik" (*back substitution*) dengan langkah-langkah berikut:

- Dari kongruensi (3), diperoleh $3 \mid (x-2)$, sehingga $x = 3s + 2$, untuk $s \in \mathbb{Z}$.
- Dengan mensubstitusikan nilai $x = 3s + 2$ ke kongruensi (4) diperoleh

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5 \text{ (karena } 3^{-1} \equiv 2 \pmod 5 \text{).} \end{aligned}$$

- Jadi diperoleh $5 \mid (s-2)$ atau $s = 5t + 2$, untuk $t \in \mathbb{Z}$.
- Oleh karena itu diperoleh $x = 3s + 2 = 3(5t+2) + 2 = 15t + 8$. Dengan mensubstitusikan nilai $x = 15t + 8$ ke kongruensi (5) diperoleh

$$\begin{aligned} 15t + 8 &\equiv 2 \pmod 7 \text{, karena } 15t + 8 \equiv t + 1 \pmod 7 \text{, maka} \\ t + 1 &\equiv 2 \pmod 7 \\ t &\equiv 1 \pmod 7 . \end{aligned}$$

- Jadi diperoleh $7 \mid (t-1)$ atau $t = 7u + 1$, untuk $u \in \mathbb{Z}$.

- Dengan demikian diperoleh $x = 15t + 8 = 15\,(7u + 1) + 8 = 105u + 23$. Atau $105|\,(x - 23)$, sehingga $x \equiv 23\,(\mathrm{mod}\,105)$.

- Dengan demikian diperoleh $x = 15t + 8 = 15\,(7u + 1) + 8 = 105u + 23$. Atau $105|\,(x - 23)$, sehingga $x \equiv 23\,(\mathrm{mod}\,105)$.
- Jadi solusi x yang memenuhi (3), (4), dan (5) adalah semua $x \in \mathbb{Z}$ yang memenuhi $x \equiv 23\,(\mathrm{mod}\,105)$. Perhatikan bahwa $105 = 3 \cdot 5 \cdot 7$.
- Tinjau bahwa x yang dicari memenuhi $1000 \leq x \leq 1100$, perhatikan bahwa

$$\begin{aligned} 1050 &\equiv 0\,(\mathrm{mod}\,105)\,, \text{ akibatnya} \\ 1073 &\equiv 23\,(\mathrm{mod}\,105)\,. \end{aligned}$$

- Dengan demikian diperoleh $x = 15t + 8 = 15\,(7u + 1) + 8 = 105u + 23$. Atau $105|\,(x - 23)$, sehingga $x \equiv 23\,(\mathrm{mod}\,105)$.
- Jadi solusi x yang memenuhi (3), (4), dan (5) adalah semua $x \in \mathbb{Z}$ yang memenuhi $x \equiv 23\,(\mathrm{mod}\,105)$. Perhatikan bahwa $105 = 3 \cdot 5 \cdot 7$.
- Tinjau bahwa x yang dicari memenuhi $1000 \leq x \leq 1100$, perhatikan bahwa

$$\begin{aligned} 1050 &\equiv 0\,(\mathrm{mod}\,105)\,, \text{ akibatnya} \\ 1073 &\equiv 23\,(\mathrm{mod}\,105)\,. \end{aligned}$$

- Jadi banyaknya prajurit yang tersisa ada sebanyak 1073 prajurit.

Teorema Sisa Tiongkok (*Chinese Remainder Theorem*)

Teorema (Teorema Sisa Tiongkok (*Chinese Remainder Theorem*))

Diberikan bilangan bulat $m_1, m_2, \ldots, m_n$ yang lebih besar dari 1 dan relatif prima sepasang demi sepasang (yaitu $\gcd(m_i, m_j) = 1$ untuk setiap $i \neq j$), apabila $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, maka sistem kongruensi linier

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

memiliki solusi tunggal dalam modulo $m = m_1 m_2 \cdots m_n$ (dengan perkataan lain, terdapat tepat satu $x \in \mathbb{Z}_m$ yang memenuhi sistem kongruensi linier tersebut).

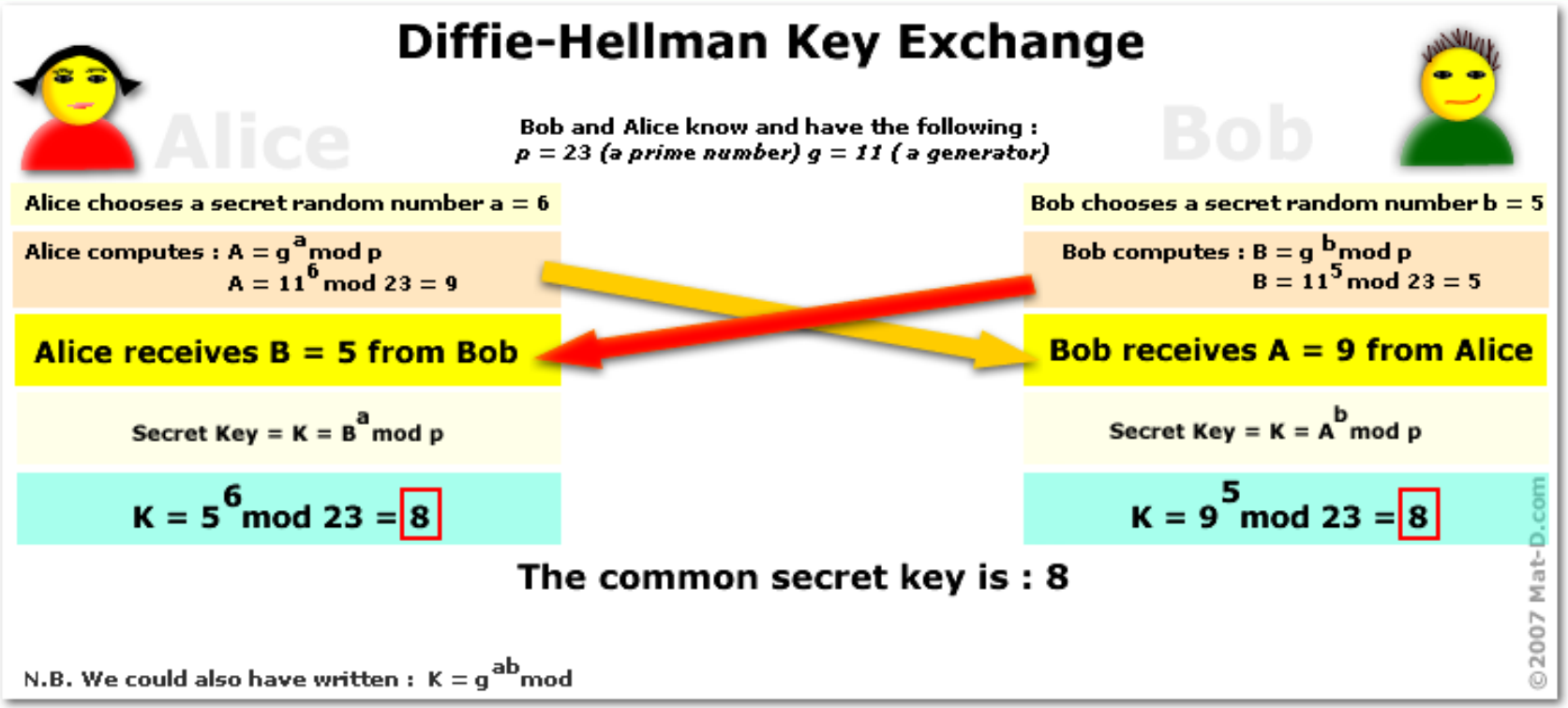
Bahasan

Mutual Password Problem

Permasalahan

Alice dan Bob ingin membuat sebuah akun yang *password*-nya hanya diketahui oleh mereka berdua. *Password* tersebut terdiri dari enam digit bilangan desimal. Awalnya mereka ingin membuat *password* tersebut bersama-sama di suatu tempat, namun Alice dan Bob tidak dapat bertemu karena mereka tinggal sangat berjauhan. Ketika mereka ingin membahas *password* bersama tersebut via *chat*/ telepon, mereka takut bila Eve, musuh mereka, menyadap pembicaraan penting yang mereka lakukan. Dapatkah Alice dan Bob membuat *password* bersama tanpa harus bertemu dan tanpa membahas secara eksplisit *password* yang digunakan dalam pembicaraan yang mereka lakukan?

Protokol Diffie-Hellman



Gambar: Gambar diambil dari http://matdonline.free.fr/img/diffieHellman.png.

Penjelasan Formal Protokol

Parameter Publik	
Pihak yang dipercaya memilih dan mengumumkan: himpunan $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ dengan p bilangan prima dan sebuah $g \in \mathbb{Z}_p^*$ dengan sifat: $\forall h \in \mathbb{Z}_p^* \; \exists k \in \mathbb{N}_0 \left(g^k = h\right)$	
Kunci Privat	
Alice	**Bob**
Pilih bilangan $a \in [0, p-1]$	Pilih bilangan $b \in [0, p-1]$
Pertukaran Kunci	
Alice menghitung $A = g^a \bmod p$ Alice mengirim A ke Bob.	Bob menghitung $B = g^b \bmod p$. Bob mengirim B ke Alice.
Perhitungan Kunci Bersama	
Alice	**Bob**
Alice menghitung $A' = B^a \bmod p$	Bob menghitung $B' = A^b \bmod p$
Kunci bersama adalah $A' = B'$.	

Keabsahan Protokol Diffie-Hellman

Tinjau bahwa

$$\begin{aligned} A' &= B^a \bmod p = \left(g^b \bmod p\right)^a \bmod p = g^{ba} \bmod p, \\ B' &= A^b \bmod p = \left(g^a \bmod p\right)^b \bmod p = g^{ab} \bmod p, \end{aligned}$$

karena $ab = ba$, maka $A' = B'$.