Bahan kuliah II4021 Kriptografi

Algoritma Pertukaran Kunci Diffie-Hellman

Oleh: Rinaldi M

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2026

Persoalan

- Misalkan Alice dan Bob sepakat menggunakan algoritma kriptografi kunci-simetri (misalnya AES) untuk enkripsi dan dekripsi pesan.

- Masalahnya, Alice dan Bob harus memiliki kunci AES yang sama untuk enkripsi dan dekripsi pesan.

- Bagaimana cara Alice dan Bob dapat berbagi kunci AES yang sama dengan aman tanpa diketahui pihak ketiga?

- Solusinya: 1) Gunakan *hybrid cryptog*raphy, atau
  2) Gunakan algoritma pertukaran kunci Diffie-Hellman

Hybrid Cryptography

- Alice dan Bob sepakat mengenkripsi dan mendekripsi pesan dengan algoritma kriptografi simetri (misalkan AES).
- Bagaimana cara Bob dapat mengetahui kunci AES yang digunakan oleh Alice (kunci AES)?
- Solusinya adalah dengan menggunakan *hybrid cryptography*.
- *Hybrid cryptography*: menggabungkan kriptografi kunci-simetri (misalkan AES) dengan kriptografi kunci-publik (misalkan RSA).
- Caranya sebagai berikut:

  1) Alice memiliki sepasang kunci privat (SK_{Alice}) dan kunci publik (PK_{Alice}) miliknya.

  2) Bob juga memiliki sepasang kunci privat (SK_{Bob}) dan kunci publik (PK_{Bob}) miliknya.

3) Alice membangkitkan kunci rahasia (K) untuk enkripsi pesan dengan AES

4) Alice mengenkripsi K dengan RSA menggunakan kunci publik Bob (PK_{Bob}).

$E\_RSA_{PKbob}(K) = CK$

5) Alice mengenkripsi pesan M dengan AES menggunakan K,

$E\_AES_{K}(M) = CM$

lalu mengirim CK dan CM kepada Bob.

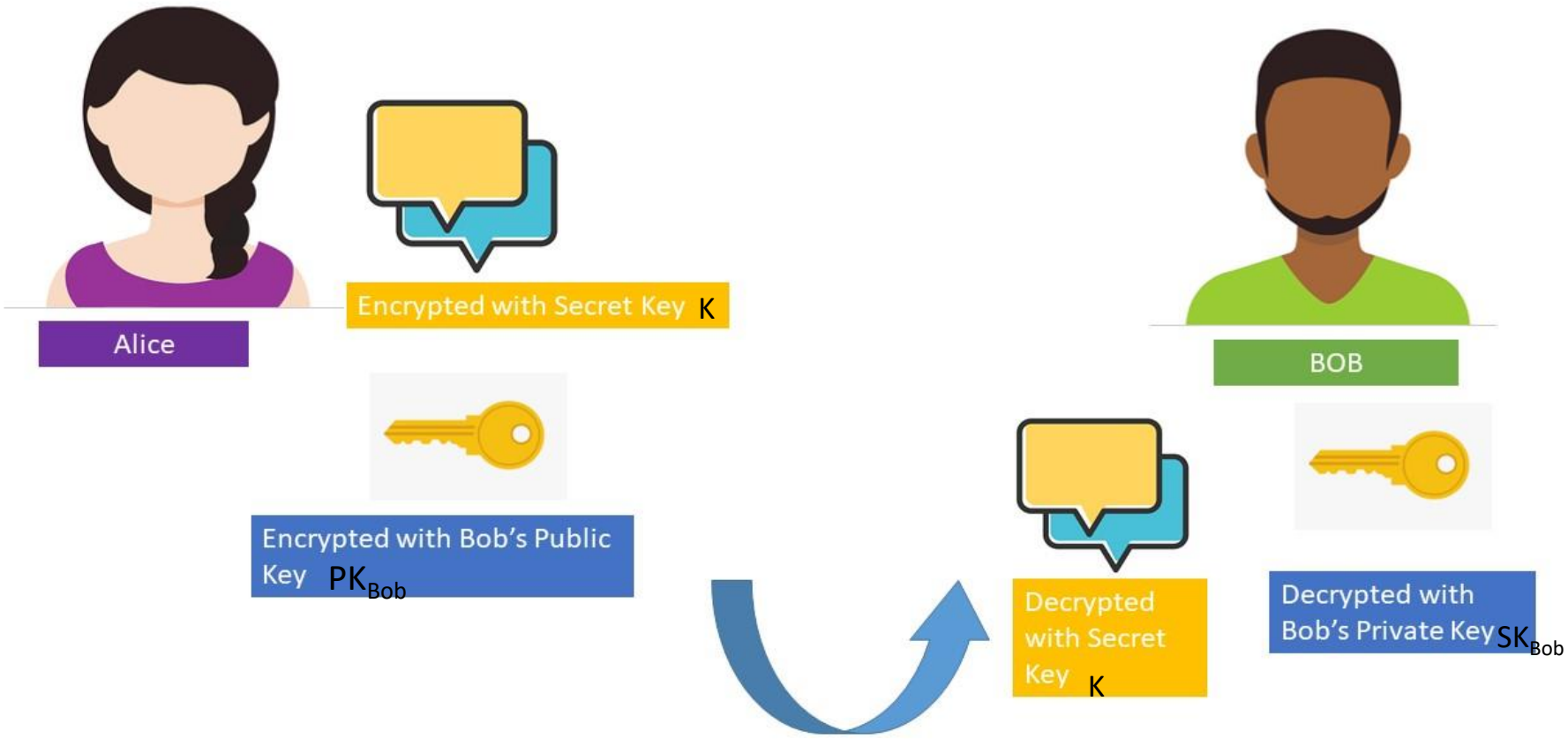
6) Bob mendekripsi CK dengan RSA menggunakan kunci privatnya (SK_{Bob})

$D\_RSA_{SKbob}(CK) = K$

7) Selanjutnya Bob mendekripsi pesan CM dengan AES menggunakan K

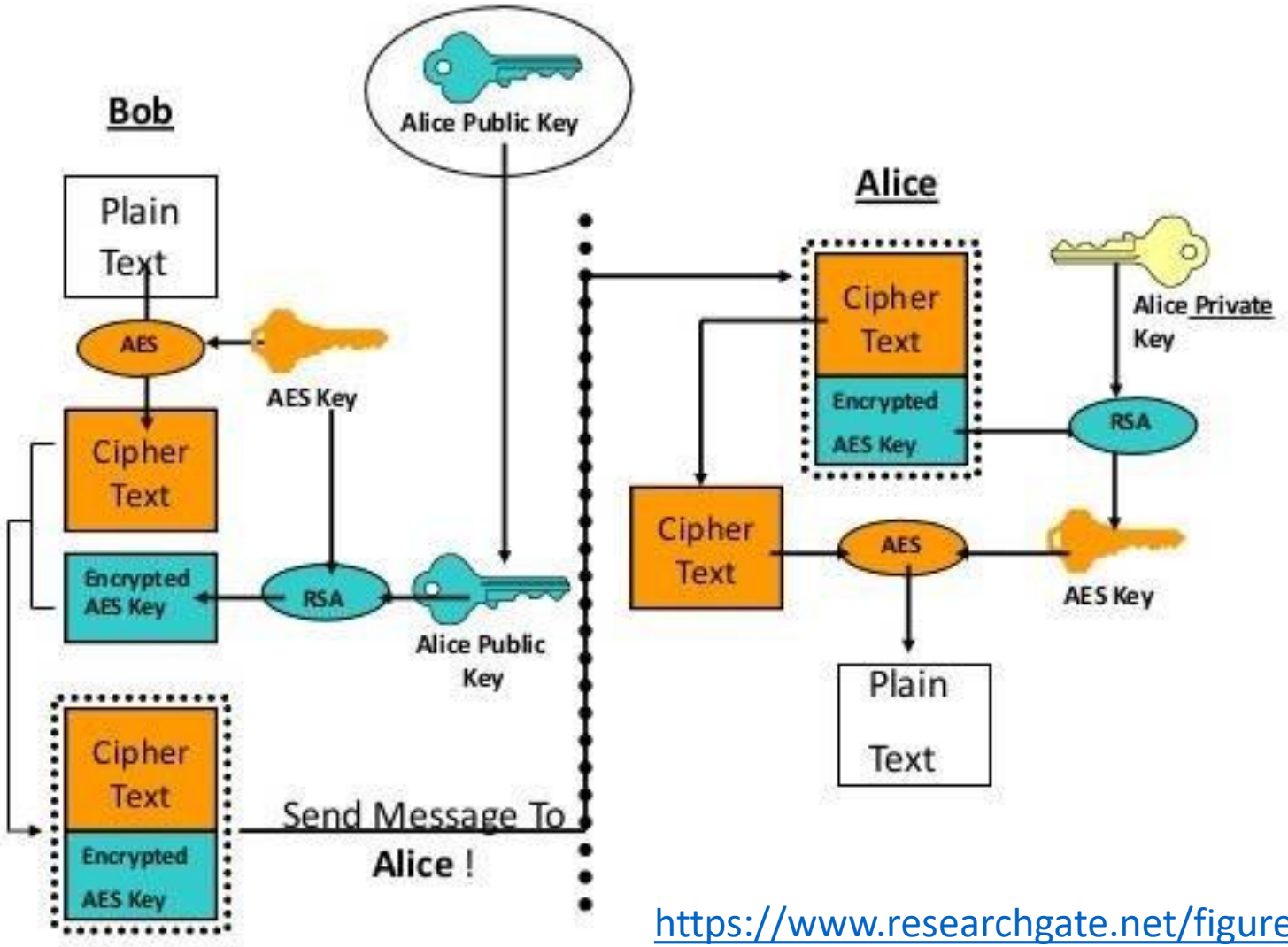
$D\_AES_{K}(CM) = M$

Hybrid Cryptography



Sumber: https://www.mayurpahwa.com/2018/12/hybrid-cryptography.html

Hybrid Cryptography



https://www.researchgate.net/figure/Illustration-of-a-hybrid-cryptosystem_fig8_327799148

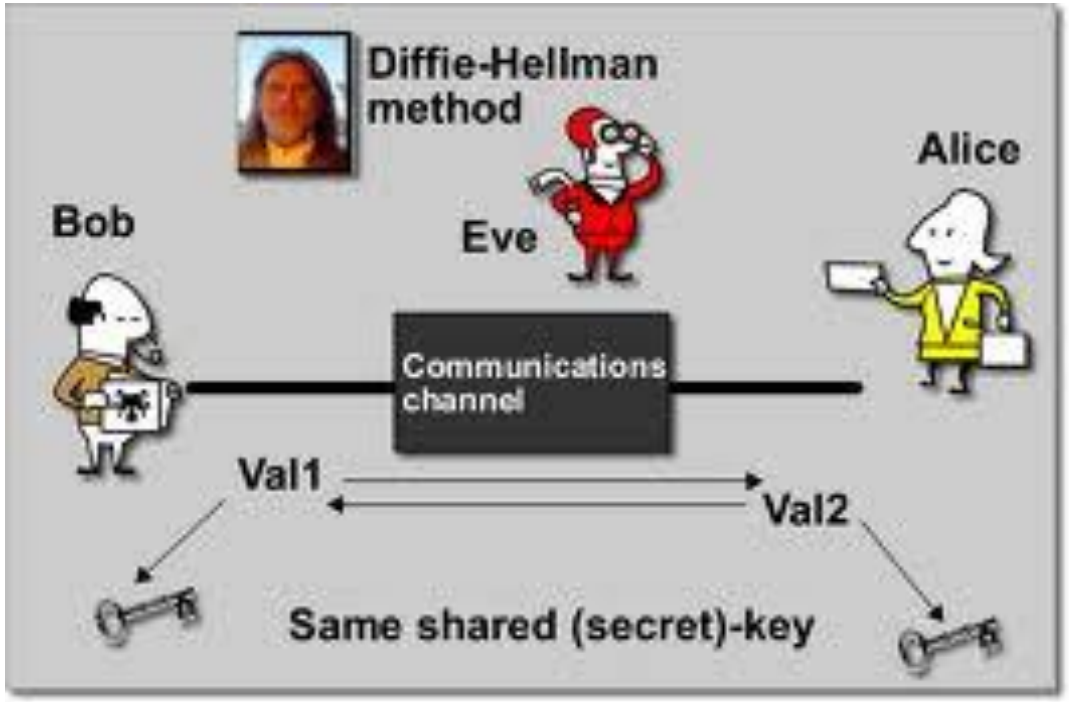
- Alternatif selain *hybrid cryptography* adalah menggunakan algoritma pertukaran kunci Diffie-Hellman.

Algoritma Pertukaran Kunci Diffie-Hellman

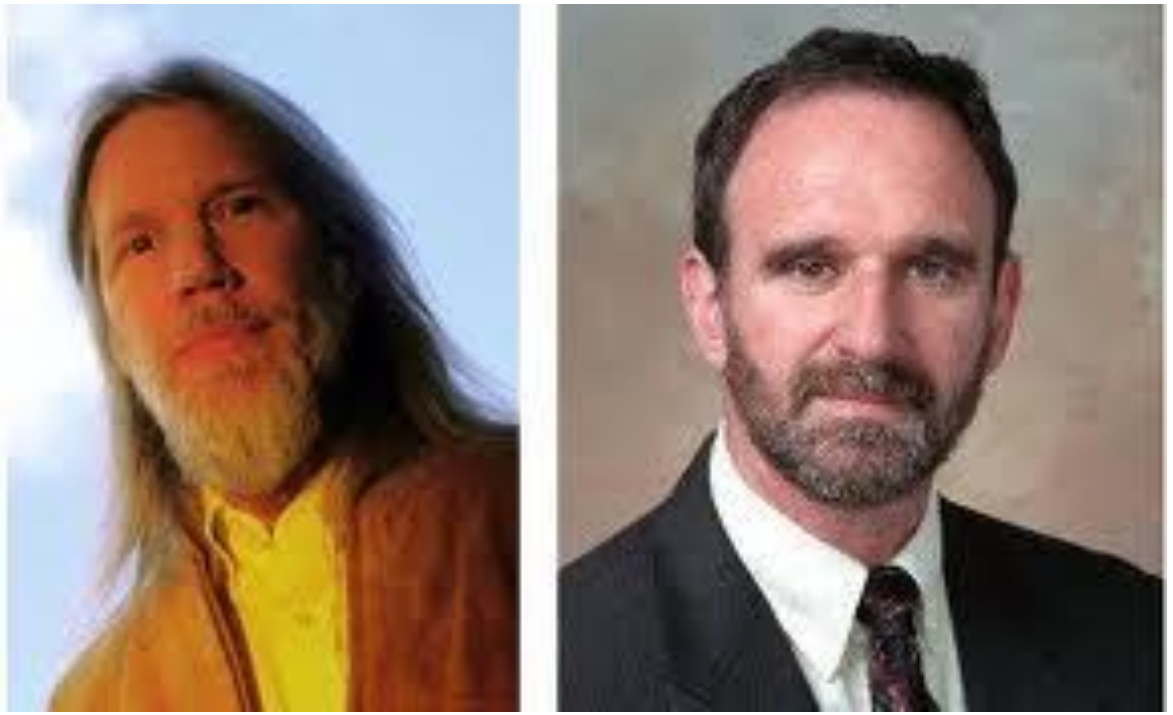
- Algoritma (lebih tepat disebut **protokol**) **pertukaran kunci Diffie-Hellman** (DH) berguna untuk berbagi kunci rahasia yang sama antara dua entitas yang berkomunikasi.

- Kunci rahasia selanjutnya digunakan untuk mengenkripsi pesan-pesan dengan algoritma kriptografi kunci-simetri (misalnya DES, AES, dll)

- Keamanan algoritma DH didasarkan pada sulit menghitung logaritma diskrit dari sebuah bilangan bulat besar.

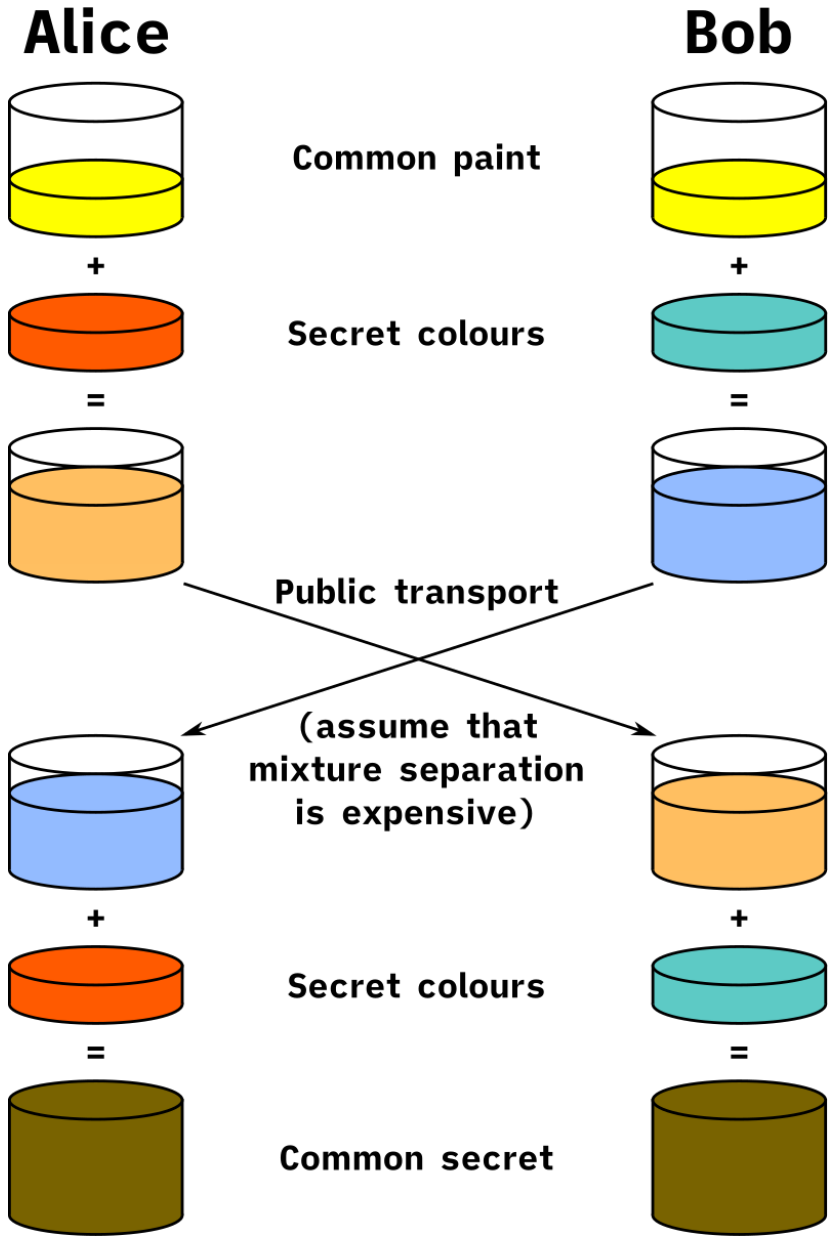


- Algoritma pertukaran kunci Diffie-Hellman dipublikasikan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976



Whitfield **Diffie** dan Martin **Hellman**

- Analogi pertukaran kunci Diffie-Hellman adalah seperti pertukaran cat antara dua orang (Alice dan Bob).
- Mula-mula Alice dan Bob menyepakati cat bersama yang warnanya tidak perlu rahasia (misalnya cat berwarna kuning)
- Masing-masing Alice dan Bob memiliki cat warna lain yang rahasia (dalam hal ini merah dan biru *cyan*)
- Alice dan Bob mencampurkan cat kuning dengan cat rahasia mereka masing-masing. Misalkan hasil pencampurannya adalah cat oranye dan cat biru terang
- Kemudian Alice dan Bob saling mempertukarkan cat hasil pencampuran tersebut (dikirim melalui transportasi umum).
- Selanjutnya, Alice dan Bob mencampurkan lagi cat rahasianya masing-masing dengan cat hasil pertukaran tersebut.
- Sekarang Alice dan Bob memilik cat berwarna sama yang rahasia.



Sumber gambar: Wikipedia

Parameter umum Diffie-Hellman

- Misalkan dua entitas yang berkomunikasi adalah Alice dan Bob.

- Mula-mula Alice dan Bob menyepakati sebuah bilangan prima p, dan sebuah bilangan bulat g, sedemikian sehingga $g < p$ dan g adalah akar primitif dari p.

- Nilai p dan g tidak perlu rahasia. Bahkan, Alice dan Bob dapat membicarakannya melalui saluran publik yang tidak aman sekalipun.

Algoritma Pertukaran Kunci Diffie-Hellman

1. Alice membangkitan bilangan bulat acak a dan mengirim hasil perhitungan berikut kepada Bob:

   $A = g^a \bmod p$ (a = kunci privat Alice, A = kunci publik Alice)

2. Bob membangkitkan bilangan bulat acak b dan mengirim hasil perhitungan berikut kepada Alice:

   $B = g^b \bmod p$ (b = kunci privat Bob, B = kunci publik Bob)

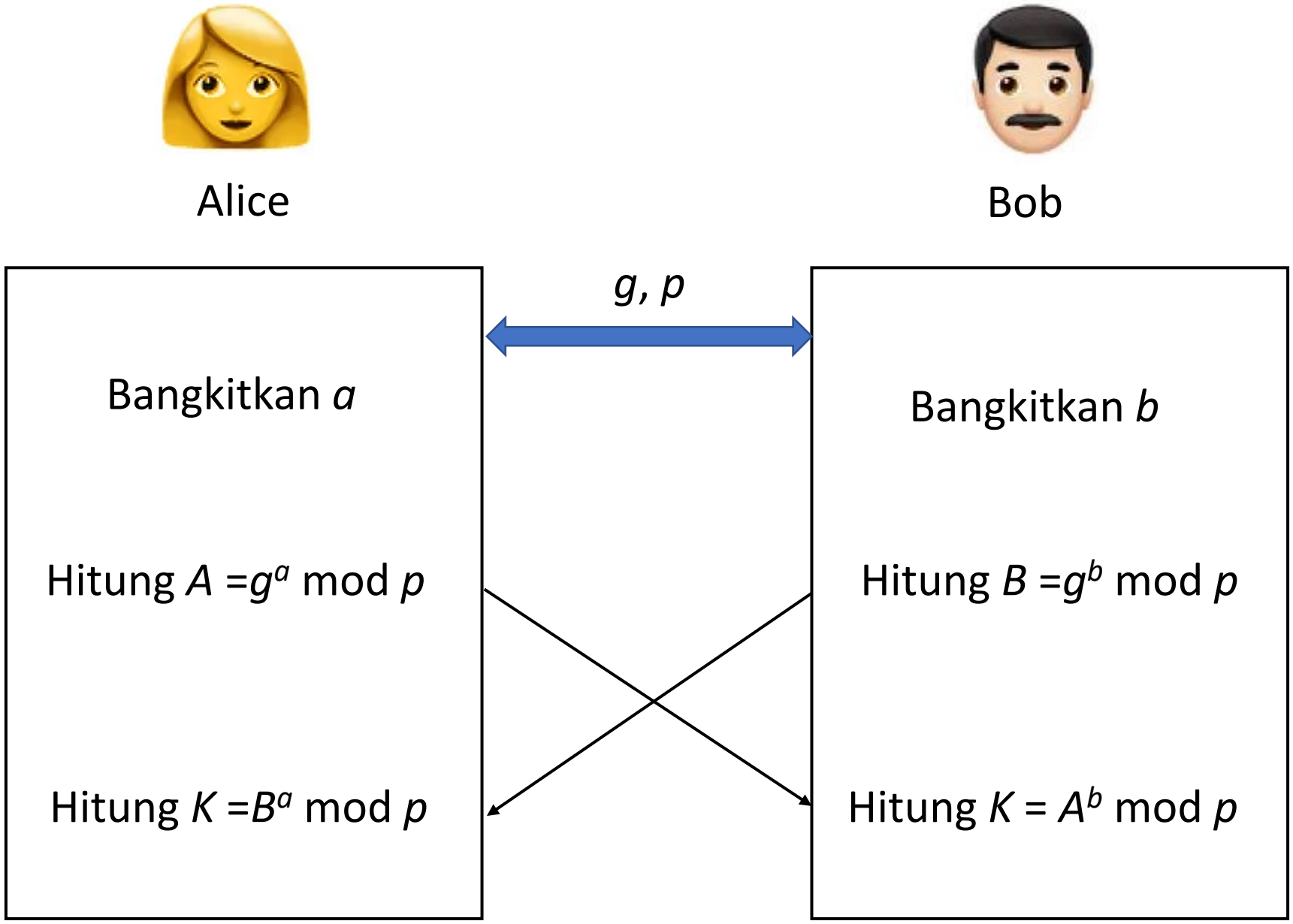
3. Alice menghitung

   $K = B^a \bmod p$ ($K = g^{ab} \bmod p$)

4. Bob menghitung

   $K = A^b \bmod p$ ($K = g^{ab} \bmod p$)

- Jika perhitungan dilakukan dengan benar, maka $K = g^{ab} \bmod p$. Alice dan Bob sekarang memiliki kunci rahasia yang sama, yaitu K.


Alice
Bob
g, p
Bangkitkan a
Hitung A =g^a mod p
Hitung K =B^a mod p
Bangkitkan b
Hitung B =g^b mod p
Hitung K = A^b mod p

- Eve (seorang kriptanalis) yang menyadap pembicaraan Alice dan Bob tidak dapat menghitung K.

- Sebab Eve hanya memiliki informasi p, g, A dan B yang semuanya tidak rahasia, tetapi ia tidak mengetahui nilai a atau b.

- Untuk mengetahui a , Eve perlu melakukan perhitungan untuk menemukan a dari persamaan $A = g^a \bmod p$. (a adalah logaritma diskrit dari A dalam modulus p)

- Sekali a diketahui, maka selanjutnya Eve menggunakannya untuk menghitung kunci rahasia $K = B^a \bmod p$.

- Kabar baiknya, logaritma diskrit bilangan bulat yang besar sangat sulit dihitung. Jadi, Eve tidak dapat menemukan kunci K.

Contoh: Alice dan Bob menyepakati $p = 353$ dan $g = 3$ ($3 < 353$, dan 3 adalah akar primitif 353)

1. Alice memilih $a = 97$ dan menghitung

   $A = g^a \bmod p = 3^{97} \bmod 353 = 40$

   Alice mengirim A kepada Bob.

2. Bob memilih $b = 233$ dan menghitung

   $B = g^b \bmod p = 3^{233} \bmod 353 = 248$

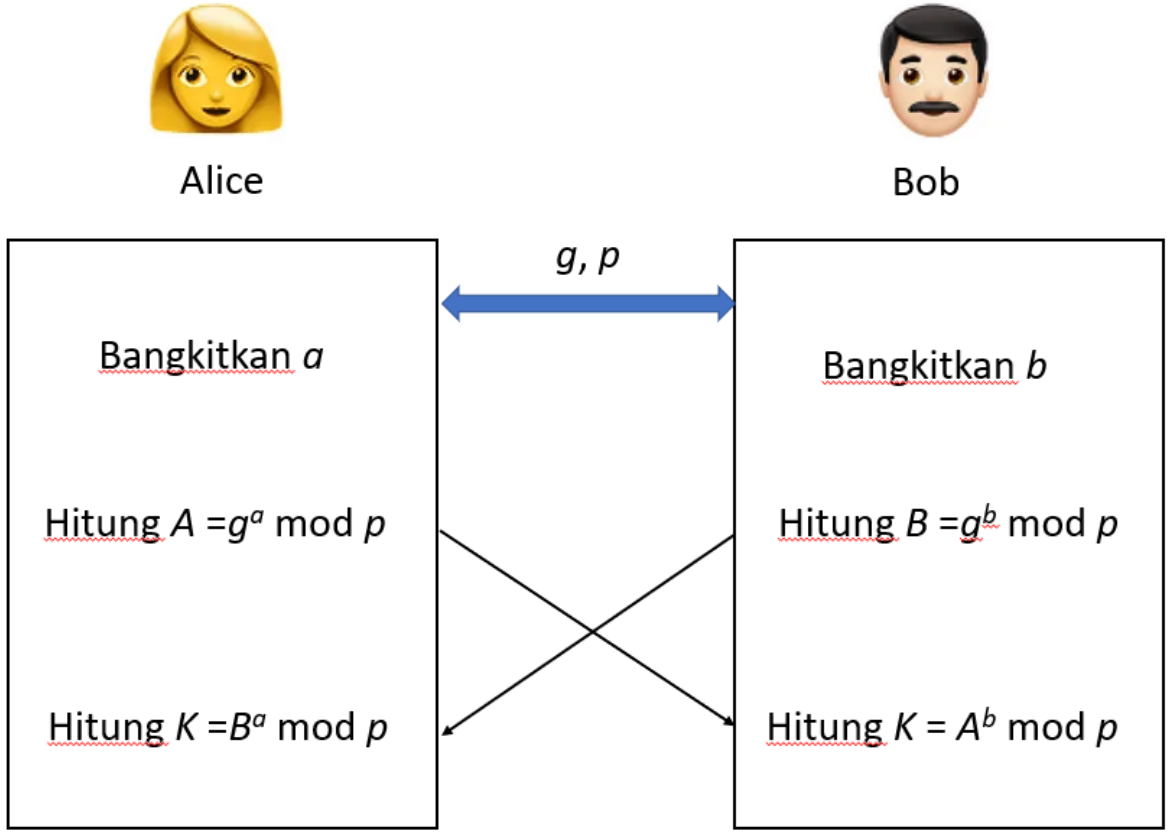
   Bob mengirim B kepada Alice.

3. Alice menghitung kunci rahasia K,

   $K = B^a \bmod p = 248^{97} \bmod 353 = 160$

4. Bob menghitung kunci rahasia K,

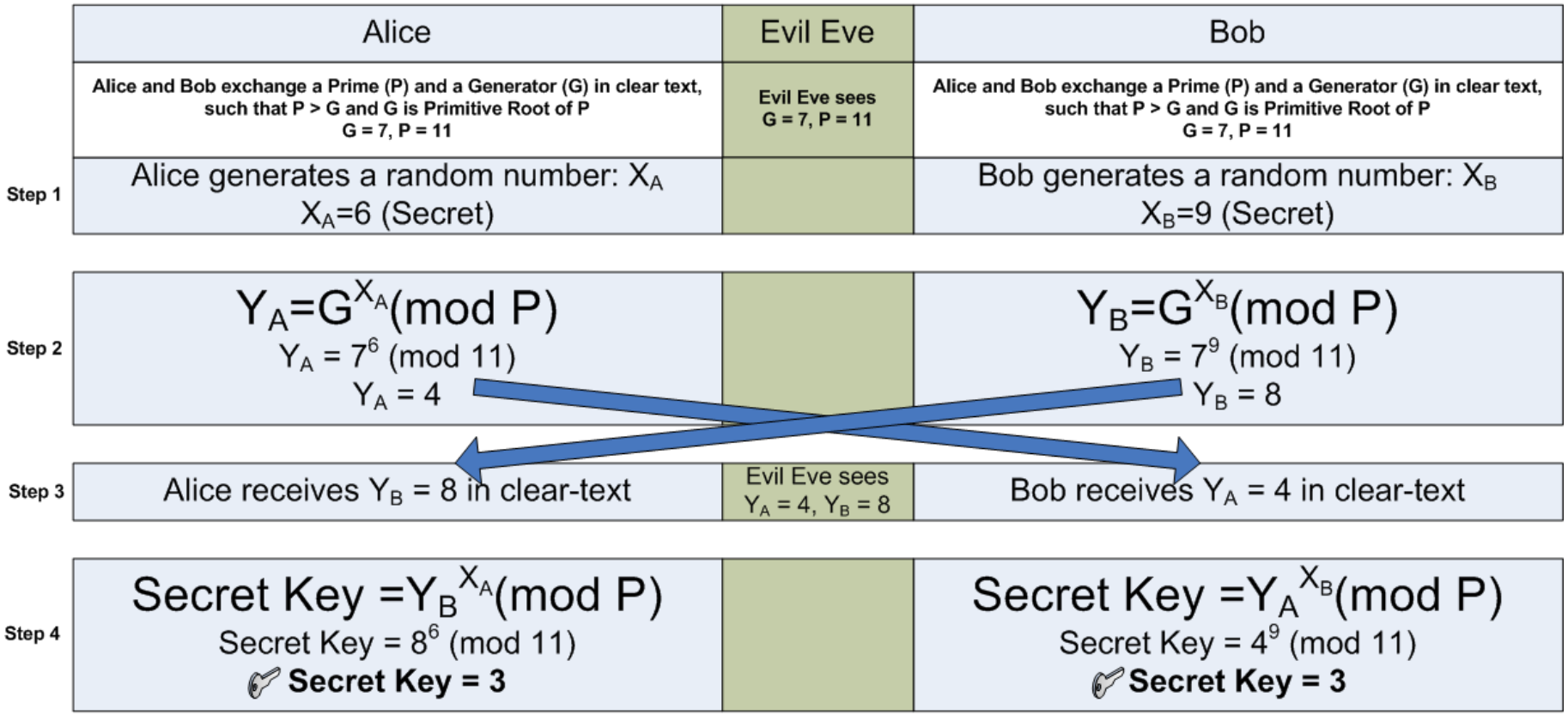
   $K = A^b \bmod p = 40^{233} \bmod 353 = 160$



Jadi, Alice dan Bob sekarang sudah mempunyai kunci rahasia yang sama, yaitu $K = 160$. Mereka dapat menggunakan K sebagai kunci enkripsi dan dekripsi pesan dengan algoritma kunci simetri.

- Contoh lain:

Diffie Hellman Key Exchange



Sumber: http://sspai.com/26497

Serangan pada Diffie-Hellman

- Pertukaran kunci Diffie-Hellman hanya aman terhadap serangan pasif, misalnya penyadapan (*eavesdropping*).
- Eva yang menyadap komunikasi antara Alice dan Bob hanya mengetahui nilai *g*, *p*, *A* dan *B* (semuanya publik). Dia tidak dapat mendeduksi *a* dan *b* (kunci privat Alice dan Bob) dari nilai-nilai publik tersebut. Untuk mendeduksi *a* dan *b*, Eva harus dapat menghitung logaritma diskrit dari persamaan $A = g^a \bmod p$ atau $B = g^b \bmod p$.

- Namun, Diffie-Hellman tidak tahan terhadap serangan aktif seperti *man-in-the-middle attack*.

- Misalkan Mallory mengintervensi komunikasi antara Alice dan Bob. Kepada Alice Malllory menyamar (*impersonation*) sebagai Bob, dan kepada Bob Mallory menyamar sebagai Alice.

- Gambar *man-in-the-middle attack* berikut memperlihatkan cara Mallory menyepakati kunci yang sama dengan Alice ($K_1 = g^{am} \bmod p$) dan menyepakati kunci yang sama dengan Bob ($K_2 = g^{bm} \bmod p$)

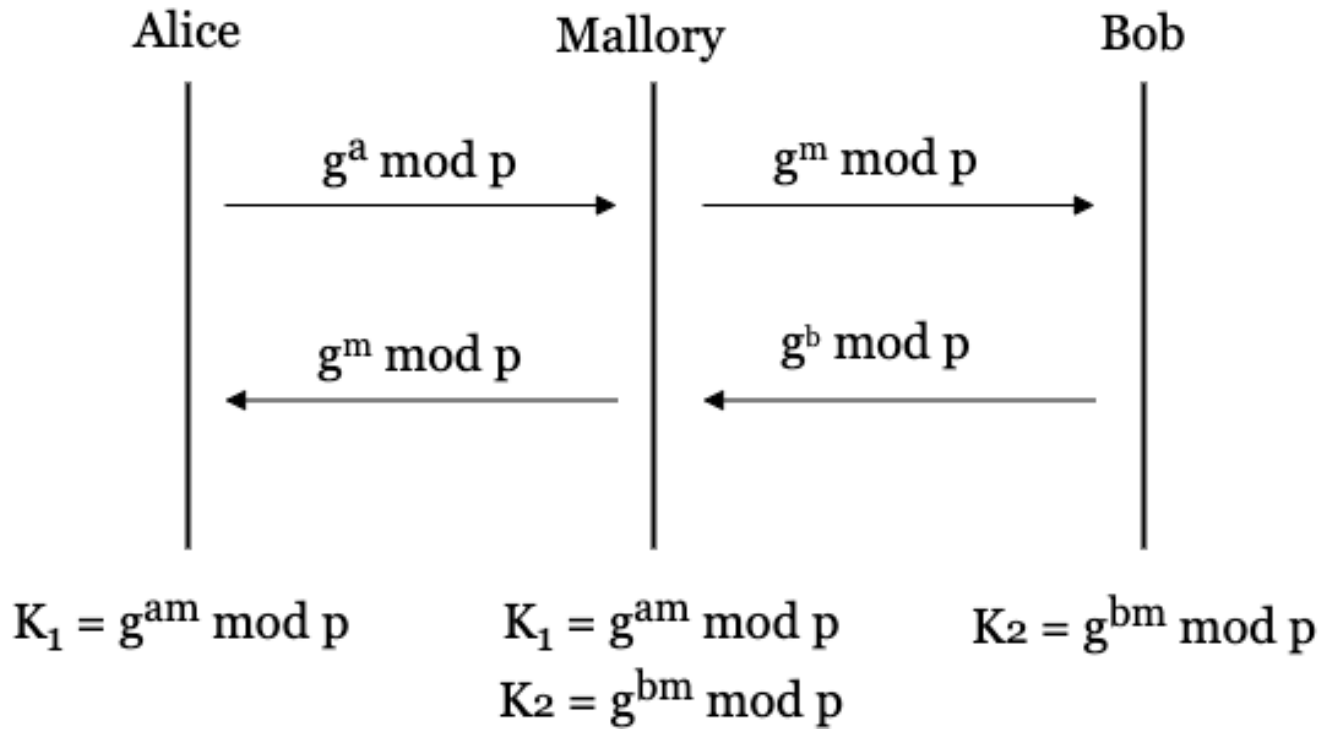
  - Ketika Alice mengirim $g^a \bmod p$ kepada Bob, Mallory mengintersepsi komunikasi dan menggantikannya dengan $g^m \bmod p$ lalu mengirimkannya kepada Bob

  - Ketika Bob mengirim $g^b \bmod p$ kepada Alice, Mallory mengintersepsi komunikasi dan menggantikannya dengan $g^m \bmod p$ lalu mengirimkannya kepada Alice.

  - Alice menghitung $K_1 = g^{am} \bmod p$, sama dengan yang dihitung Mallory, $K_1 = g^{am} \bmod p$

  - Bob menghitung $K_2 = g^{bm} \bmod p$, sama dengan yang dihitung Mallory, $K_2 = g^{bm} \bmod p$

  - Selanjutnya Mallory mengetahui pesan2 rahasia dari Alice dan dari Bob yang diekripsi dengan dengan kunci K_1 dan K_2 tersebut



Sumber gambar: https://textbook.cs161.org/crypto/key-exchange.html

Pertukaran kunci Diffie-Hellman untuk tiga pihak (Alice, Bob, dan Carol)

1. Alice, Bob, dan Carol menyepakati *p* dan *g*.
2. Alice, Bob, dan Carol membangkitkan kunci privat masing-masing, *a*, *b*, dan *c*.
3. Alice menghitung $\boldsymbol{g^a \bmod p}$ dan mengirimkannya kepada Bob.
4. Bob menghitung $\boldsymbol{(g^a)^b \bmod p = g^{ab} \bmod p}$ dan mengirimkannya kepada Carol.
5. Carol menghitung $\boldsymbol{K = (g^{ab})^c \bmod p = g^{abc} \bmod p}$.
6. Bob menghitung $\boldsymbol{g^b \bmod p}$ dan mengirimkannya kepada Carol.
7. Carol menghitung $\boldsymbol{(g^b)^c \bmod p = g^{bc} \bmod p}$ dan mengirimkannya kepada Alice.
8. Alice menghitung $\boldsymbol{K = (g^{bc})^a \bmod p = g^{bca} \bmod p = g^{abc} \bmod p}$.
9. Carol menghitung $\boldsymbol{g^c \bmod p}$ dan mengirimkannta kepada Alice.
10. Alice menghitung $\boldsymbol{(g^c)^a \bmod p = g^{ca} \bmod p}$ dan mengirimkannya kepada Bob.
11. Bob menghitung $\boldsymbol{K = (g^{ca})^b \bmod p = g^{cab} \bmod p = g^{abc} \bmod p}$.
12. Sekarang Alice, Bob, dan Carol sudah memiliki kunci rahasia yang sama, yaitu *K*

- Algoritma Diffie-Hellman dipakai di dalam protokol SSL dan TLS. SSL/TLS digunakan untuk mengamankan komunikasi di internet antara *client* dan *server*.

- Pada tahun 2002, Hellman menyarankan algoritma DH diberi nama algoritma pertukaran kunci **Diffie–Hellman–Merkle** sebagai penghargaan terhadap kontribusi Ralph Merkle dalam penemuan kriptografi kunci-publik:

- Hellman menulis:

  The system...has since become known as Diffie–Hellman key exchange. While that system was first described in a paper by Diffie and me, it is a public key distribution system, a concept developed by Merkle, and hence should be called 'Diffie–Hellman–Merkle key exchange' if names are to be associated with it. I hope this small pulpit might help in that endeavor to recognize Merkle's equal contribution to the invention of public key cryptography.[7]

  Sumber: Wikipedia

The IEEE Koji Kobayashi Computers and Communications Award

The 1999 award was given to Diffie, Hellman and Merkle for "For the revolutionary invention of public key cryptosystems which form the foundation for privacy, integrity and authentication in modern communication systems."

The 2000 award was given to Rivest, Shamir and Adleman "For the revolutionary invention of the RSA public key cryptosystem which is the first to be widely-adopted."

From left to right: Adi Shamir, Ron Rivest, Len Adleman, Ralph Merkle, Martin Hellman, and Whit Diffie (Picture courtesy of Eli Biham, taken at the presentation on Monday August 21 at Crypto 2000, an IACR conference

Sumber: http://www.merkle.com/merkleDir/KobayashiAward.html

Demo DH online: https://asecuritysite.com/encryption/diffie