II4031 Kriptografi dan Koding

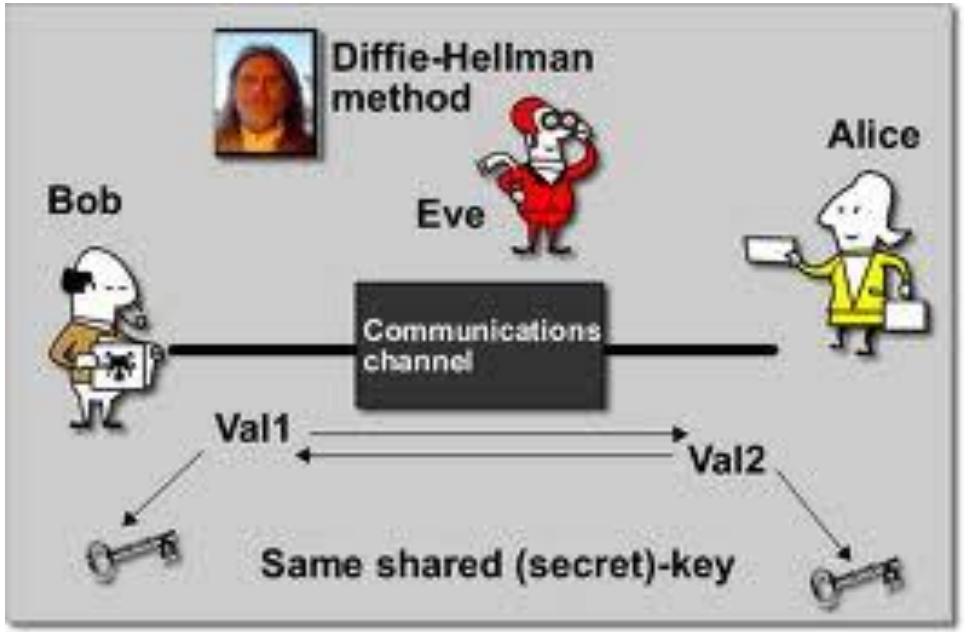
Algoritma Pertukaran Kunci Diffie-Hellman

Oleh: Rinaldi Munir

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
ITB

Latar Belakang

- Kegunaan: untuk berbagi kunci rahasia yang sama antara dua entitas yang berkomunikasi. Kunci rahasia digunakan untuk mengenkripsi pesan dengan algoritma kriptografi kunci-simeteri (DES, AES, dll)



- Keamanan algoritmanya didasarkan pada sulitnya menghitung logaritma diskrit.


Whitfield **Diffie** and Martin **Hellman**

Parameter umum Diffie-Hellman

- Misalkan dua orang yang berkomunikasi: Alice dan Bob.

- Mula-mula Alice dan Bob menyepakati bilangan prima yang besar, n dan g, sedemikian sehingga $g < n$.

- Bilangan n dan g tidak perlu rahasia. Bahkan, Alice dan Bob dapat membicarakannya melalui saluran yang tidak aman sekalipun.

Algoritma Pertukaran Kunci Diffie-Hellman

1. Alice membangkitan bilangan bulat acak yang besar *x* dan mengirim hasil perhitungan berikut kepada Bob:

   $X = g^x \bmod n$

2. Bob membangkitkan bilangan bulat acak yang besar *y* dan mengirim hasil perhitungan berikut kepada Alice:

   $Y = g^y \bmod n$

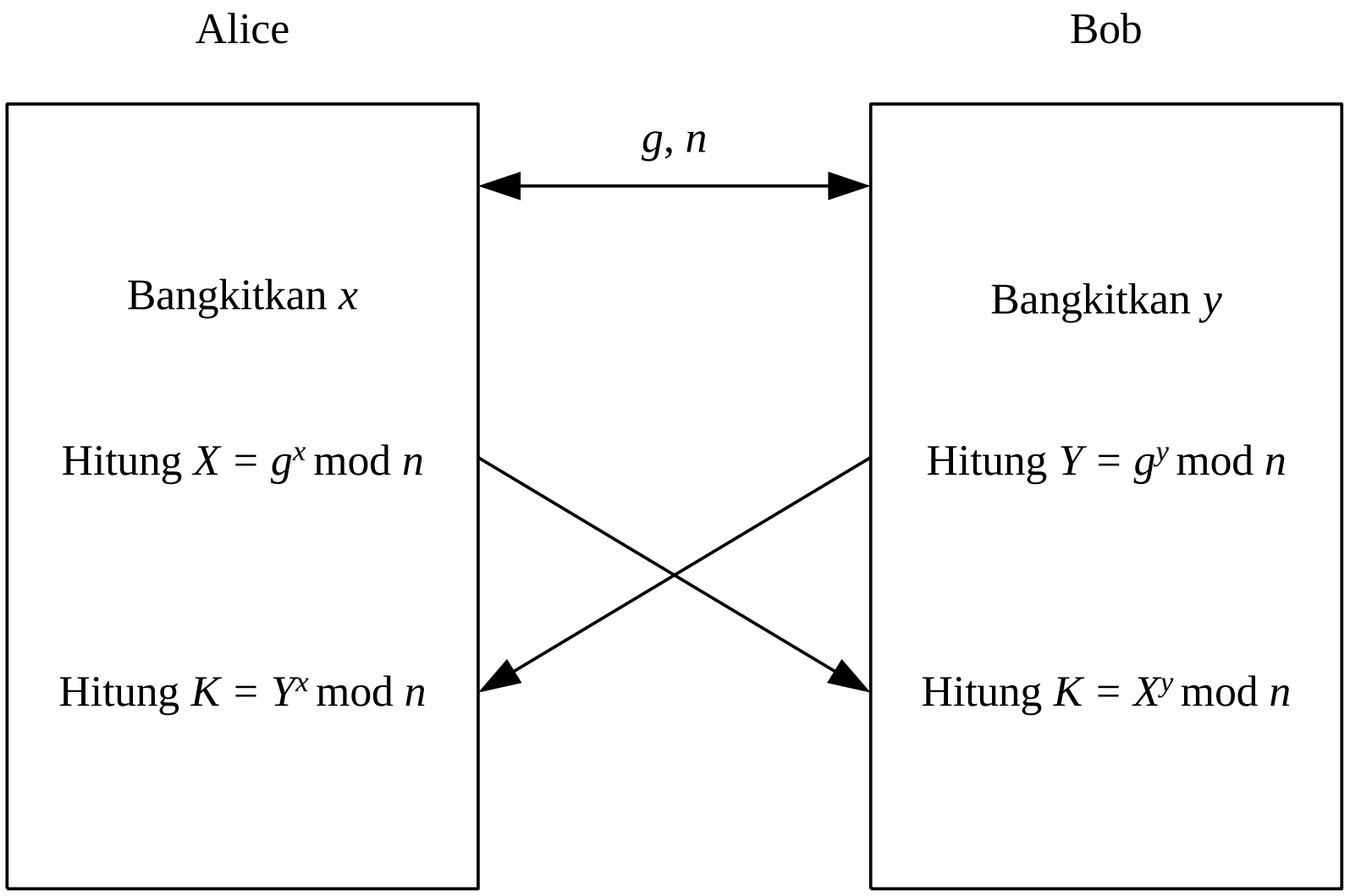
3. Alice menghitung

   $K = Y^x \bmod n$

4. Bob menghitung

   $K' = X^y \bmod n$

- Jika perhitungan dilakukan dengan benar, maka $K = K'$. Baik K dan $K' = g^{xy} \bmod n$.


Alice
Bob
g, n
Bangkitkan x
Hitung X = g^x mod n
Hitung K = Y^x mod n
Bangkitkan y
Hitung Y = g^y mod n
Hitung K = X^y mod n

Eve (seorang kriptanalis) yang menyadap pembicaraan antara Alice danBob tidak dapat menghitung K.

- Eve hanya memiliki informasi n, g, X dan Y (yang tidak rahasia), tetapi ia tidak mempunyai informasi nilai x atau y.

- Untuk mengetahui x , Eve perlu melakukan perhitungan untuk menemukan x dari persamaan $X = g^x \bmod n$.

- Sekali x diketahui, maka selanjutnya Eve menggunakannya untuk menghitung kunci $K = Y^x \bmod n$.

- Kabar baiknya, logaritma diskrit sangat sulit dihitung.

Contoh: Alice dan Bob menyepakati $n = 97$ dan $g = 5$ ($g < n$)

1. Alice memilih $x = 36$ dan menghitung

   $X = g^x \bmod n = 5^{36} \bmod 97 = 50$

   Alice mengirim X kepada Bob.

2. Bob memilih y = 58 dan menghitung

   $Y = g^y \bmod n = 5^{58} \bmod 97 = 44$

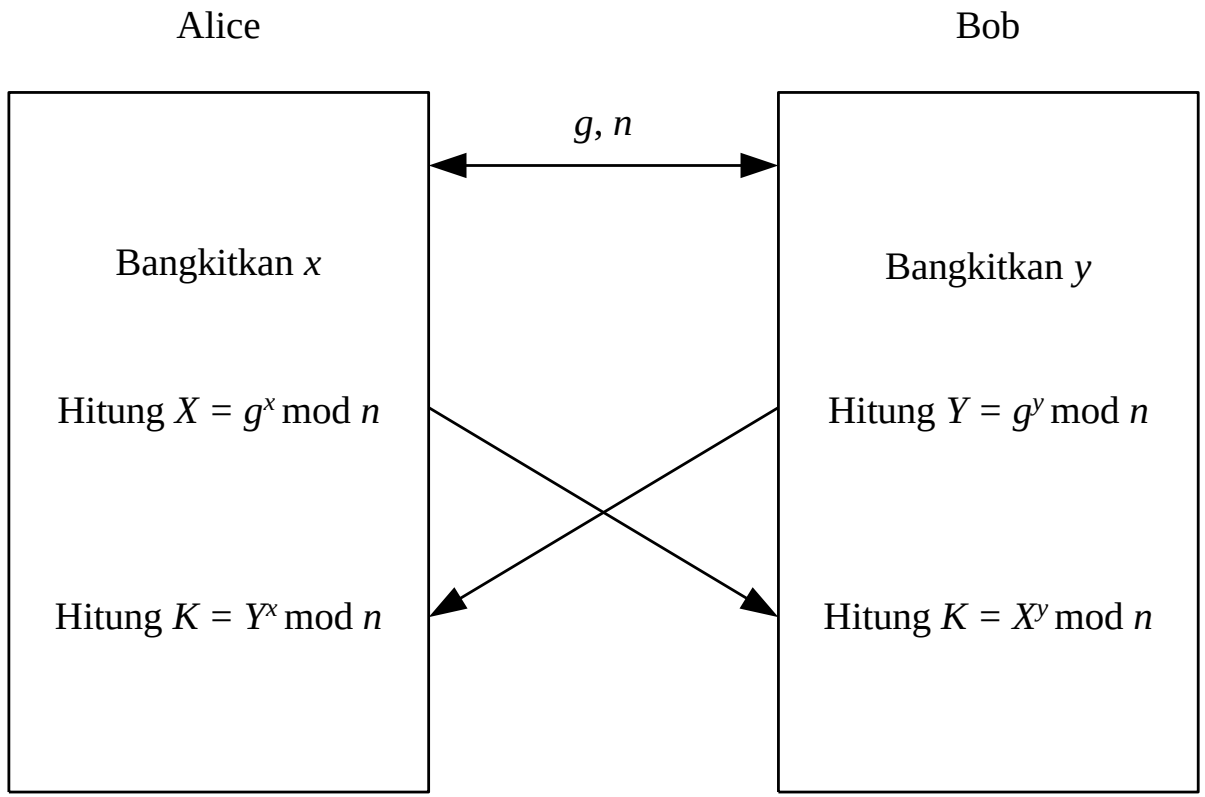
   Bob mengirim Y kepada Alice.

3. Alice menghitung kunci simetri K,

   $K = Y^x \bmod n = 44^{36} \bmod 97 = 75$

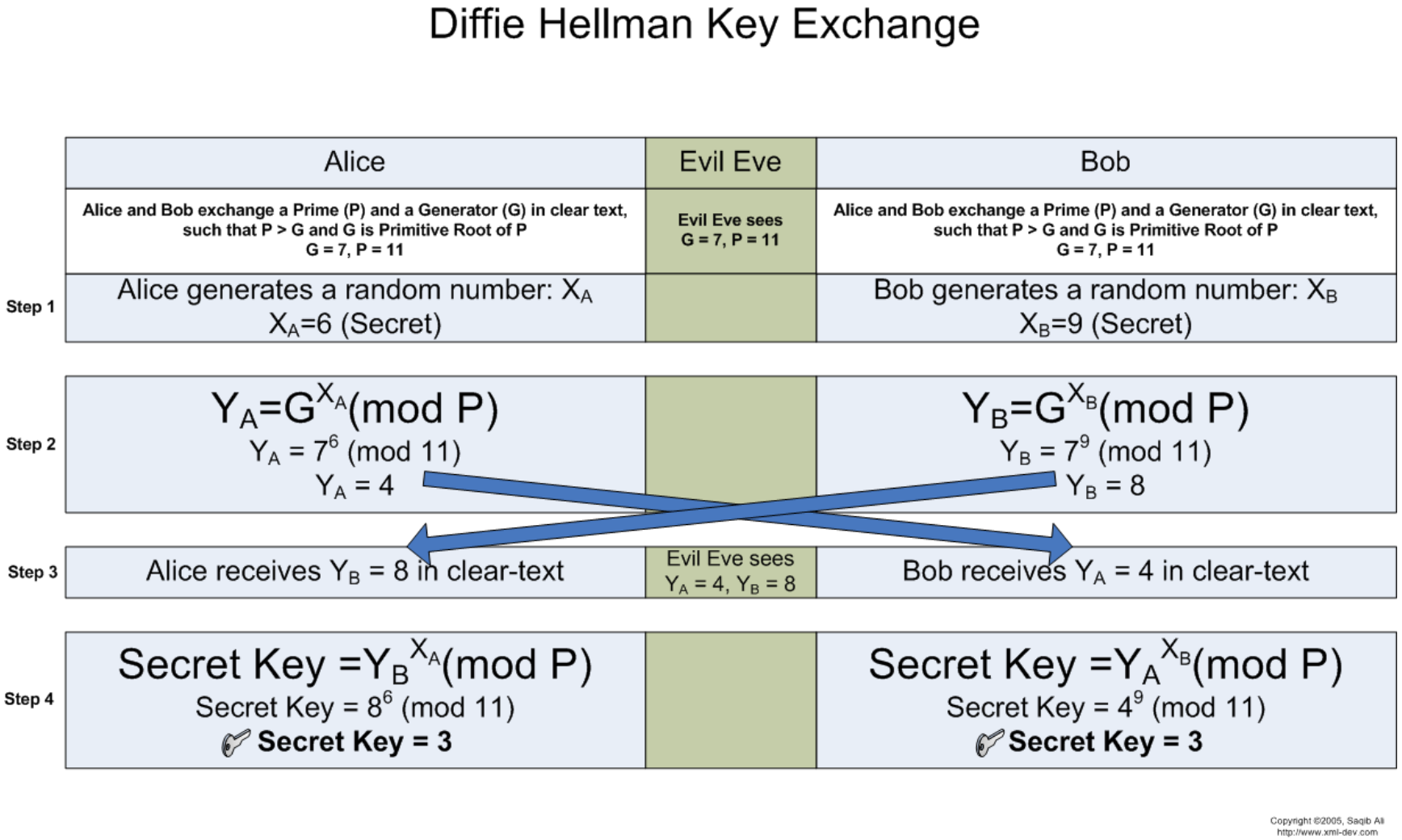
4. Bob menghitung kunci simetri K,

   $K = X^y \bmod n = 50^{58} \bmod 97 = 75$



Jadi, Alice dan Bob sekarang sudah mempunyai kunci enkripsi simetri yang sama, yaitu $K = 75$.

- Contoh lain:



Sumber: http://sspai.com/26497

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