AES And Diffie-Hellman

Student : SHANG-TING,SHIE (數三 謝尚庭)
Po-Chen Chen (數三 陳柏臣)

Advisor : Prof . Pin-Chi Hung (洪斌哲 教授)

What is AES ?

Advanced Encryption Standard (AES) is Symmetric-key algorithm which is a method when you already have an encryption key, you can find the corresponding decryption key easily, and it became effective as a U.S. federal government standard on May 26, 2002.

What is Diffie-Hellman ?

Diffie–Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric-key cipher.

Using AES Method To Encryption And Decryption

Let f(x) be irreducible polynomial in $Z_2[x]$, $\frac{Z_2(x)}{<f(x)>}$ is a quotient ring .

- Plaintext => m(x)
- Inverse of g(x) => h(x) ***By Euclidean algorithm*** **[g · h ≡ 1 , mod f]**
- Choose => g(x), g(x) ≠ 0
- Ciphertext => c(x)

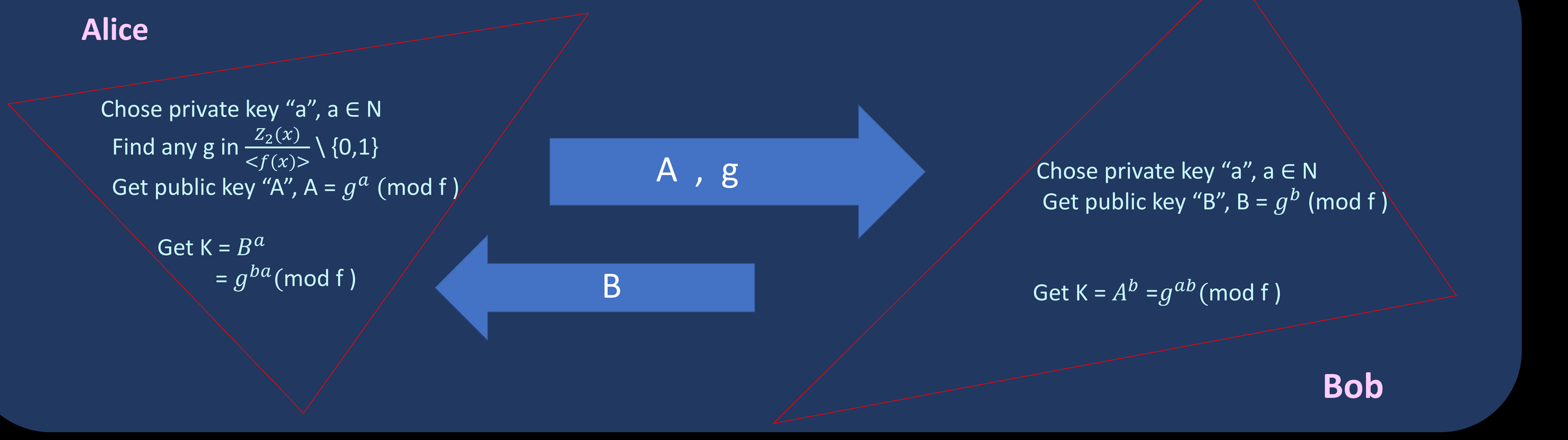
Where m(x),g(x),h(x),c(x) ∈ $\frac{Z_2(x)}{<f(x)>}$

Step1
Encryption => m · g mod f ≡ c

Step2
Find inverse of g => h

Step3
Decryption => c · h mod f ≡ m

AES Key Exchange



Building on Discrete Logarithm problem for $\frac{Z_2(x)}{<f(x)>}$ \ {0}.

The complexity of our AES key exchange is the same with the D-H key exchange.

Security **Efficiency**