School of InfoComm Technology ict Taking IT Higher

NGEE ANN POLYTECHNIC

CRYPTOGRAPHY (CTG)

Diploma in Cybersecurity and Digital Forensics (Dip in CSF)

Academic Year (AY) `21/`22 – Semester 2

WEEK 13.1

DIFFIE–HELLMAN KEY EXCHANGE (DHE)

Last Updated: 22/11/2020

Diffie–Hellman Key Exchange: Overview

- Proposed in 1976 by Whitfield Diffie and Martin Hellman
- Widely used, e.g. in Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPSec)
- The Diffie–Hellman Key Exchange (DHKE) is a key exchange protocol and not used for encryption

Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Diffie–Hellman Key Exchange: Overview

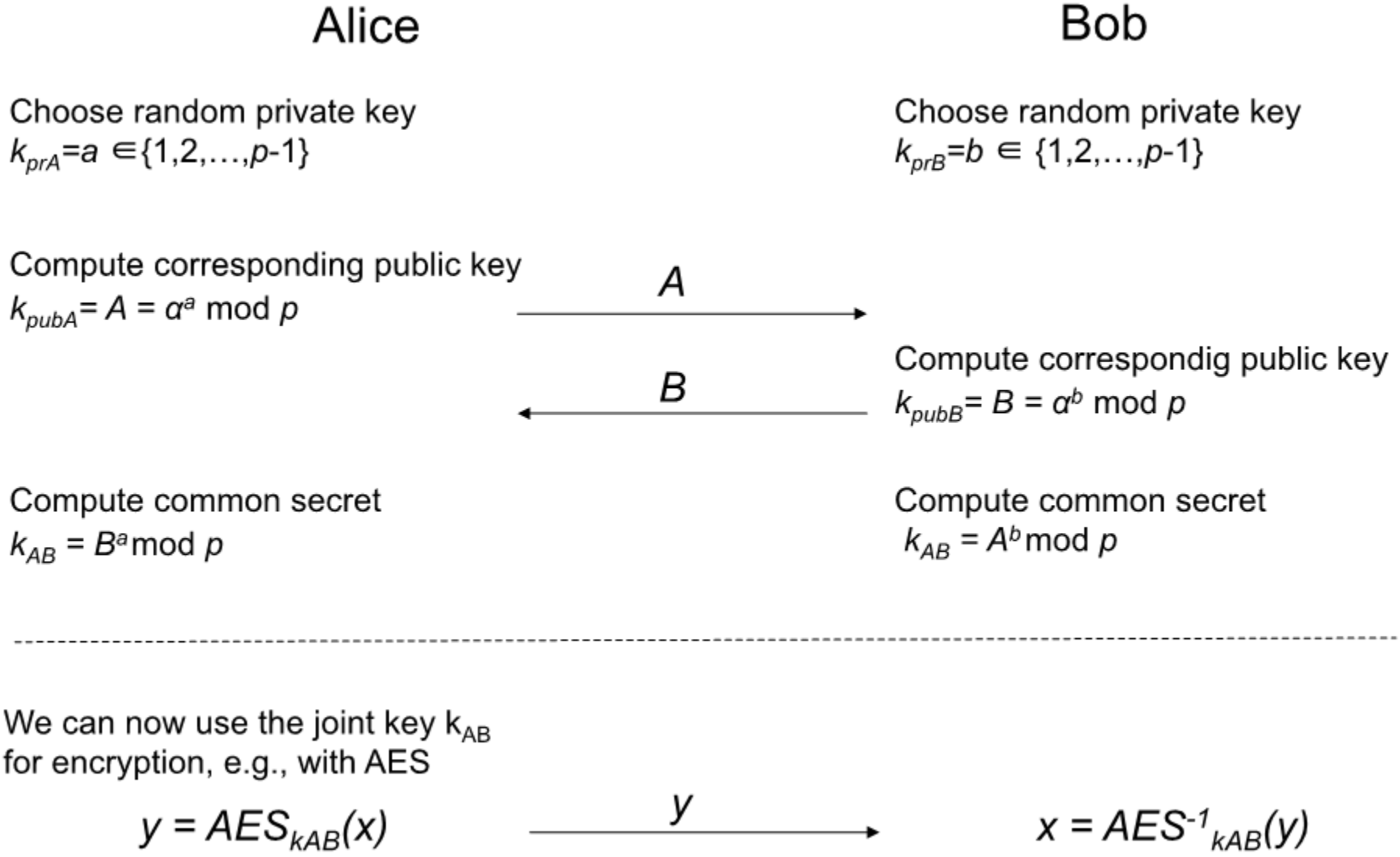
- The question of key exchange was one of the first problems addressed by a cryptographic protocol.
- This was prior to the invention of public key cryptography.
- The Diffie-Hellman key agreement protocol was the first practical method for establishing a shared secret over an unsecured communication channel.
- The point is to agree on a key that two parties can use for a symmetric encryption, in such a way that an eavesdropper cannot obtain the key.

Diffie–Hellman Key Exchange: Set-up

- 1. Choose a large prime p.
- 2. Choose an integer $\alpha \in \{2,3, \ldots, p-2\}$.
- 3. Publish p *and* α.

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Diffie–Hellman Key Exchange



Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Diffie–Hellman Key Exchange: Example

Domain parameters p=29, α=2

Alice		Bob
Choose random private key $k_{prA} = a = 5$		Choose random private key $k_{prB} = b = 12$
Compute corresponding public key $k_{pubA} = A = 2^5 \bmod 29 = 3$	$A = 3$ →	
	← $B = 7$	Compute correspondig public key $k_{pubB} = B = 2^{12} \bmod 29 = 7$
Compute common secret $k_{AB} = B^a \bmod 29 = 7^5 \bmod 29 = 16$		Compute common secret $k_{AB} = A^b \bmod 29 = 3^{12} \bmod 29 = 16$

Proof of correctness:

Alice computes: $B^a \bmod p$
Bob computes: $A^b \bmod p$

i.e., Alice and Bob compute the same key k_{AB}!

The Discrete Logarithm Problem

Discrete Logarithm Problem (DLP) in Z_p^*

- Given is the finite cyclic group Z_p^* of order $p-1$ and a primitive element $\alpha \in Z_p^*$ and another element $\beta \in Z_p^*$.
- The DLP is the problem of determining the integer $1 \leq x \leq p-1$ such that $\alpha^x \equiv \beta \bmod p$
- This computation is called the **discrete logarithm problem (DLP)**

$$x = log_\alpha \beta \bmod p$$

- Example: Compute x for $5^x \equiv 41 \bmod 47$

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Attacks against the Discrete Logarithm Problem

- In order to prevent attacks that compute the DLP, it is recommended to use primes with a length of at least 1024 bits for schemes such as Diffie-Hellman
- A prime p with 1024 bits; in base 10 that would be about 308 digits. An example, expressed in hexadecimal, is

- p= de9b707d 4c5a4633 c0290c95 ff30a605 aeb7ae86 4ff48370 f13cf01c 49adb9f2 3d19a439 f743ee77 03cf342d 87f43110 5c843c78 ca4df639 931f3458 fae8a94d 1687e99a 76ed99d0 ba87189f 42fd31ad 8262c54a 8cf5914a e6c28c54 0d714a5f 6087a172 fb74f481 4c6f968d 72386ef3 45a05180 c3b3c7dd d5ef6fe7 6b0531c3

- z= 56c03667 f3b50335 ad532d0a dcaa2897 a02c0878 099d8e3a ab9d80b2 b5c83e2f 14c78cee 664bce7d 209e0fd8 b73f7f68 22fcdf6f fade5af2 ddbb38ff 3d2270ce bbed172d 7c399f47 ee9f1067 f1b85ccb ec8f43b7 21b4f980 2f3ea51a 8acd1f6f b526ecf4 a45ad62b 0ac17551 727b6a7c 7aadb936 2394b410 611a21a7 711dcde2

- To compute with huge integers like these, you need a special "multiple precision" software package, because the built-in arithmetic on computer chips handles only 32 or 64 bits.

Exercises

Diffie–Hellman Key Exchange: Example

- $p = 23, \alpha = 5, a = 6, b = 15$
  - $A = ?$
  - $B = ?$
  - $K_{AB} = ?$
- $p = 11, \alpha = 2, a = 9, b = 4$
  - $A = ?$
  - $B = ?$
  - $K_{AB} = ?$

Summary

Summary

- You learnt
  - Diffie–Hellman Key Exchange
  - The Discrete Logarithm Problem