● Diffie-Hellman 키 교환

1. 알고리즘 절차

단 계	행위자	세부 내용
준 비	공 통	• 송수신자는 두 수 p와 g를 선택한다. • p는 매우 **큰 소수**이다.(10진수 300자리 이상 되도록 한다) • g는 Z_p^*의 원소 중에서 임의의 **원시근**을 선택하도록 한다. • 선택된 p와 g를 네트워크상에 공개되어도 무방하다. • (p, g)를 네트워크상에서 전송한다. • 송수신자는 (p, g)를 네트워크상에서 합의할 수 있다.
교 환	A → B	• A는 0≤x≤p-1 범위에서 임의의 x를 선택한다.**(x는 비밀유지)** • 그리고, **a = g^x mod p**를 계산한다. • A는 x값은 자신만의 비밀로 하고, B에게는 계산한 a를 보낸다.
	B → A	• B는 0≤y≤p-1 범위에서 임의의 y를 선택한다.**(y는 비밀유지)** • 그리고, **b = g^y mod p**를 계산한다. • B는 y값은 자신만의 비밀로 하고. A에게는 계산한 b를 보낸다.
공통키 생 성	A	• A는 자신만의 **비밀값 x**를 이용하여 다음을 계산한다. • $K_A = b^x \bmod p$를 계산한다. → b는 B에게서 받은 값이다.
	B	• B는 자신만의 **비밀값 y**를 이용하여 다음을 계산한다. • $K_B = a^y \bmod p$를 계산한다. → a는 A에게서 받은 값이다.
결 론	• A와 B가 구한 값은 같은 값이 된다. • 즉, $K_A = K_B$가 된다.**(K_A, K_B는 비밀유지)** • A와 B는 x, y 값을 모르면서 동일한 키 값을 얻게 된다. • K_A와 K_B는 같은 값으로 **공통 비밀키(대칭키)**가 된다.	
분 석	• 송수신자가 공유하는 대칭키는 **K = g^{xy} mod p**이다.**(k는 비밀유지)**	

Diffie-Hellman 키 교환에서 송수신자가 공유하는 대칭키는 K = g^{xy} mod p이다.

예제

Diffie-Hellman 키 교환 알고리즘 예제

앞에서 소개한 "Diffie-Hellman 키 교환 알고리즘" 절차만을 공부해서는 이해하기 어렵다.

다음 예제를 보면 쉽게 이해될 수 있다.

① 먼저, 송수신자는 두 수 p와 g를 선택한다. p=13, g=7이 선택된 것으로 한다.

② 송신자 A
- A는 0≤x≤p-1 범위에서 임의의 x를 선택한다. **x=3**을 선택**(x는 비밀유지)**
- $a = g^x \bmod p$를 계산한다.
- $a = 7^3 \bmod 13 = 343 \bmod 13 =$ **5** → B에게 **a=5**를 전송

③ 수신자 B
- B는 0≤y≤p-1 범위에서 임의의 y를 선택한다. **y=2**를 선택**(y는 비밀유지)**
- $b = g^y \bmod p$를 계산한다.
- $b = 7^2 \bmod 13 = 49 \bmod 13 =$ **10** → A에게 **b=10**을 전송

서로 교환

④ 송신자 A : $K_A = b^x \bmod p = 10^3 \bmod 13 = 1000 \bmod 13 =$ **12**

⑤ 수신자 B : $K_B = a^y \bmod p = 5^2 \bmod 13 = 25 \bmod 13 =$ **12**

⑥ 결론
- A와 B가 구한 값은 같다. 즉, $K_A = K_B =$ **12**가 된다.
- A와 B는 서로 x, y 값을 모르면서 **동일한 값 12**를 얻게 된다.
- 값 **12**가 송수신자가 **공유하는 비밀키(대칭키)**가 된다.

⑦ 분석
- 송수신자가 공유하는 대칭키는 $K = g^{xy} \bmod p$이다.
- $K = g^{xy}$ **mod p** $= 7^{3 \cdot 2} \bmod 13 = 117649 \bmod 13 =$ **12(비밀유지)**

⑧ Diffie-Hellman 키 교환에서 같은 값을 가지는 수식 - 중요!

- $K_A = b^x \bmod p = 10^3 \bmod 13 = 1000 \bmod 13 =$ **12** → 대칭키(비밀키)
- $K_B = a^y \bmod p = 5^2 \bmod 13 = 25 \bmod 13 =$ **12**
- $K = g^{xy} \bmod p = 7^{3 \cdot 2} \bmod 13 = 117649 \bmod 13 =$ **12**

2. Diffie-Hellman 키 교환 알고리즘 분석

디피-헬만 키 교환은 키-분배센터(KDC) 없이 대칭 세션키를 생성할 수 있는 방법이다.
통신하는 두 사람은 공개된 통신망을 통해 공통의 비밀키를 공유할 수 있다.

값(정보)	세부 내용
공개된 값	• 두 수 p와 g • p는 매우 큰 **소수**이다.(10진수 300자리 이상) • g는 Z_p^*의 원소 중에서 임의의 **원시근**이다.
송신자만이 알고 있는 값	• x : 0≤x≤p-1 범위에서 임의의 x를 선택한다.**(x는 비밀)**
수신자만이 알고 있는 값	• y : 0≤y≤p-1 범위에서 임의의 y를 선택한다.**(y는 비밀)**
송수신자가 주고받는 값	• $a = g^x \bmod p$ → g^x은 공격자가 알 수 없다. • $b = g^y \bmod p$ → g^y은 공격자가 알 수 없다. ☞ x, y 값을 공격자는 모르므로 g^x, g^y의 값을 공격자는 알 수 없다. a, b 값은 공격자가 알 수 있다.
공격자가 얻을 수 있는 값	• 두 수 p와 g • $a = g^x \bmod p$ • $b = g^y \bmod p$
비밀키를 계산에 필요한 값	• x 또는 y의 값 • x 또는 y의 값을 알기 위해서는 다음을 계산해야 한다. $a = g^x \bmod p$ → **지수** x가 **이산대수**이다. $b = g^y \bmod p$ → **지수** y가 **이산대수**이다. • p 값이 충분히 크면 지수(이산대수) x, y를 구하는 것은 수학적으로 불가능하다고 알려져 있다. • 이를 "**이산대수문제 해결의 어려움**"이라 한다.

3. Diffie-Hellman 키 교환 정리

① Diffie-Hellman 키 교환은 **이산대수** 기반이다.

② Diffie-Hellman 키 교환은 암호 알고리즘이 아니다.
- Diffie-Hellman 키 교환은 그냥, **키 교환 알고리즘**이다.
- 해서, Diffie-Hellman 키 교환은 평문을 암호문으로 변경할 수 없다.
- 디피-헬만 키 교환은 비대칭키 기반의 암호 알고리즘이 아니다.
- 디피-헬만 키 교환에서 생성되는 키는 **대칭키**이다.

③ 디피-헬만 키 교환은 키-분배센터(KDC) 없이 송수신자들이 사용할 키를 생성한다.
- 키-분배센터(KDC) 없이 세션키를 생성하는 것을 "**대칭키 합의**"라 한다.
- 디피-헬만 키 교환은 KDC 없이 **대칭키(비밀키)**를 교환하는 하나의 원리이다.
- 송수신자는 공개된 통신망에서 **공통의 비밀키**를 생성하여 공유할 수 있다.

④ 디피-헬만 키 교환은 **암호학**적 통신 방법의 **기초**를 수립하였다.
- 디피와 헬만이 1976년에 발표하였고
- 디피-헬만 키 교환은 공개키 암호 알고리즘에 많은 영향을 주었다.
- 1977년, 공개키 암호 알고리즘인 RSA 암호가 발표되었다.

4. 국-대-국 프로토콜(station-to-station protocol)

① 국-대-국 프로토콜은 디피-헬만 키 교환에 기반을 둔 프로토콜이다.
- 국-대-국 프로토콜은 디피-헬만 키 교환처럼 세션키를 공유하기 위한 것이다.

② 국-대-국 프로토콜은 **중간자 공격을 방지하기 위하여 인증**을 사용한다.
- 송수신자 사이에 세션키를 생성할 때 공개키 인증서를 이용한 전자서명을 한다.
- 전자서명은 서로를 인증하는데 사용될 수 있다.

③ 국-대-국 프로토콜에서 공개키 기반의 인증서를 사용할 경우
- 중간 공격자는 송수신자의 개인키를 알 수 없다.
- 메시지를 변조하면 공개키 검증에 실패하게 된다.
- 공격자가 송수신자의 개인키를 모르는 상태에서 메시지를 변조해도 의미가 없다.

Diffie-Hellman 키 교환의 안전성 분석

디피-헬만 키 교환은 다음 2가지 공격에 대해 취약점을 가진다.

- **이산대수 공격**
- **중간자 공격(man in the middle attack, MITM)**

---

1. 이산대수 공격

① 디피-헬만 키 교환은 "**이산대수문제 풀기 어려움**"에 기반을 둔다.

② 공격자는 통신망에서 다음 2가지 내용을 가로챌 수는 있다.

$a = g^x \bmod p$ → 여기서 x를 구하고
$b = g^y \bmod p$ → 여기서 y를 구한다.

- x, y를 구할 수 있다면 공격자는 대칭키 "$K = g^{xy} \bmod p$"를 찾을 수 있다.
- 그런데, p 값이 충분히 크면 x, y를 구하는 것은 현실적으로 불가능하다.

③ 디피-헬만 키 교환에서 이산대수 공격으로부터 안전성 조건 - 권장 사항
- p는 매우 큰 소수이어야 한다.(10진수로 300자리 이상)
- p를 선택할 때, p-1이 최소한 하나의 큰 소인수를 가지도록 선택한다.
- 큰 소인수는 10진수로 60자리 이상이 되도록 한다.
- 인수 중에서 소수인 것을 소인수(素因數, prime factor)라 한다.
- g는 Z_p^*의 원소 중 임의의 원시근에서 선택하도록 한다.
  → 다르게 표현하면, 생성자 g는 연산이 곱셈인 군 $\langle Z_p^*, \times \rangle$에서 선택하도록 한다.
  → 원시근을 생성자 또는 생성원이라 한다.(원시근에 대해서는 이론 교재 정수론 참조)
  → 원시근은 mod p의 지수연산 결과가 1부터 p-1까지의 모든 정수가 등장한다.
- 송수신자는 대칭키(비밀키)를 생성한 뒤에는 x, y 값을 폐기하도록 한다.
- x, y 값은 한번만 사용하도록 한다.

2. 중간자 공격(man in the middle attack, MITM)

① 디피-헬만 키 교환에 대한 공격 방법이 전혀 없는 것은 아니다.
- 중간자 공격으로 비밀키를 계산할 수 있다.
- 중간자 공격에서는 x, y 값을 구할 필요가 없다.
- 디피-헬만 키 교환은 수학적으로 안전하다고 할 수 있을 뿐이다.

② 중간자 공격은 통신 연결에서 송수신자 사이에 중간자가 침입하는 것이다.
- 송수신자는 모두 상대방에게 연결되었다고 생각하지만,
- 실제로는 두 사람은 중간자에게 연결되어 있다.
- 중간자는 한쪽에서 전달된 정보를 도청, 조작한 후 다른 쪽으로 전달한다.

◉ 디피-헬만 키 교환에서 중간자 공격

---

① 송신자 A는 x를 선택하고, $a = g^x \bmod p$를 계산하여, 이를 수신자 B에게 보낸다.
② 공격자 C는 중간에서 $a = g^x \bmod p$를 확보하고, 이를 보관한다.
→ 공격자 C는 z를 선택하고, $c = g^z \bmod p$를 계산하여, 이를 **송수신자**에게 보낸다.
③ 수신자 B는 y를 선택하고, $b = g^y \bmod p$를 계산하여, 이를 송신자 A에게 보낸다.
→ 공격자 C가 중간에서 $b = g^y \bmod p$를 확보하고, 송신자 A는 이를 받지 못한다.
④ 송신자와 공격자는 $K1 = g^{xz} \bmod p$를 계산한다.
→ K1은 송신자와 공격자가 공유하는 비밀키가 된다.
→ 송신자 A는 키 K1이 자신과 수신자 B와 공유하는 키로 착각한다.
⑤ 수신자와 공격자는 $K2 = g^{yz} \bmod p$를 계산한다.
→ K2는 수신자와 공격자가 공유하는 비밀키가 된다.
→ 수신자 B는 키 K2가 자신과 송신자 A와 공유하는 키로 착각한다.
⑥ 2개의 키 "K1과 K2"가 생성된다.
- K1 : 송신자와 공격자 사이에 사용되는 비밀키
- K2 : 수신자와 공격자 사이에 사용되는 비밀키

- 중간자 공격을 방지하기 위해서는 **인증**을 사용하면 된다.
- 중간자 공격을 방지하기 위한 다양한 알고리즘이 개발되어 있다.

기출문제 분석

1. Diffie-Hellman 알고리즘은 비밀키를 공유하는 과정에서 특정 공격에 취약할 가능성이 존재한다. 다음 중 Diffie-Hellman 알고리즘에 가장 취약한 공격으로 옳은 것은? [2015년 서울 9급]

① DDoS(Distributed Denial of Service) 공격
② 중간자 개입(Man-in-the-middle) 공격
③ 세션 하이재킹(Session Hijacking) 공격
④ 강제지연(Forced-delay) 공격

♤ **Diffie-Hellman 알고리즘의 취약점 – 2가지**

- 이산대수 공격 : 디피-헬만 키 교환은 "이산대수문제 풀기 어려움"에 기반을 두므로
- 중간자 공격(man in the middle attack) : 중간자 공격으로 비밀키를 계산할 수 있으므로

정답 : ②

2. Diffie-Hellman 키 교환 알고리즘에 대한 설명으로 옳은 것은? [2017년 국회 9급]

① 공개된 채널을 통하여 서로 정보를 교환하는 것만으로 공통의 비밀키를 만들 수 있다.
② 부인방지를 제공하는 전자서명이 가능하다.
③ 인수분해 문제 기반한 알고리즘이다.
④ 중간자 공격을 수행하는 것이 불가능하다.
⑤ 키 생성 시 사용된 난수가 노출되어도 비밀키는 안전하다.

♤ **Diffie-Hellman 키 교환 알고리즘**

② 부인방지를 제공하는 전자서명이 가능하다.(×)
→ Diffie-Hellman 키 교환은 암호 알고리즘이 아니므로 전자서명은 불가능하다.
③ 인수분해 문제 기반한 알고리즘이다.(×)
→ Diffie-Hellman 키 교환은 이산대수 문제 기반한 알고리즘이다.
④ 중간자 공격을 수행하는 것이 불가능하다.(×)
→ Diffie-Hellman 키 교환 알고리즘은 중간자 공격에 취약하다.
⑤ 키 생성 시 사용된 난수가 노출되어도 비밀키는 안전하다.(×)
→ 송수신자가 선택하는 난수 x, y는 비밀을 유지해야 한다.

정답 : ①

3. 키 교환 알고리즘인 Diffie-Hellman 알고리즘에 대한 설명으로 가장 옳지 않은 것은? [2020년 서울 7급]

① 이 알고리즘의 안전성은 이산대수를 계산하는 어려움에 기초한다.
② 대칭키를 공유하기 위해 사용한다.
③ 중간자 공격에 대해 강한 안정성을 가진다.
④ 실제로 키를 교환하는 것이 아니고, 공유할 키를 각자 계산하여 만들어내는 것이다.

♤ Diffie-Hellman 키 교환 알고리즘

// 디피-헬만 키 교환은 다음 2가지 공격에 대해 취약점을 가진다.

- **이산대수 공격**
- **중간자 공격**(man in the middle attack, MITM)

↓

↓중간자 공격 방지

↓

- 중간자 공격을 방지하기 위해서는 **인증**을 사용하면 된다.
- 중간자 공격을 방지하기 위한 다양한 알고리즘이 개발되어 있다.

// Diffie-Hellman 키 교환 정리

① 디피-헬만 키 교환은 **이산대수 기반**이다.
② 디피-헬만 키 교환은 **대칭키를 공유**하기 위해 사용한다.
→ 디피-헬만 키 교환은 암호 알고리즘이 아니다.(그냥, 키 교환 알고리즘이다)
→ 디피-헬만 키 교환은 비대칭키 기반의 암호 알고리즘이 아니다.
③ 디피-헬만 키 교환은 **실제로 키를 교환하는 것이 아니다.**
→ 디피-헬만 키 교환은 **공유할 키를 각자 계산하여 만들어내는 것**이다.
④ 디피-헬만 키 교환은 키-분배센터(KDC) 없이 송수신자들이 사용할 키를 생성한다.
- 키-분배센터(KDC) 없이 세션키를 생성하는 것을 "대칭키 합의"라 한다.
- 디피-헬만 키 교환은 KDC 없이 대칭키(비밀키)를 교환하는 하나의 원리이다.
- 송수신자는 공개된 통신망에서 공통의 비밀키를 생성하여 공유할 수 있다.

⑤ 디피-헬만 키 교환은 암호학적 통신 방법의 기초를 수립하였다.
- 디피와 헬만이 1976년에 발표하였고
- 디피-헬만 키 교환은 공개키 암호 알고리즘에 많은 영향을 주었다.
- 1977년, 공개키 암호 알고리즘인 RSA 암호가 발표되었다.

정답 : ③

4. 소수 p=13, 원시근 g=2, 사용자 A와 B의 개인키가 각각 3, 2일 때, Diffie-Hellman 키 교환 알고리즘을 사용하여 계산한 공유 비밀키는? [2020년 국가 9급]

① 6 ② 8
③ 12 ④ 16

♤ Diffie-Hellman 키 교환 알고리즘

① 먼저, 송수신자는 소수 p와 원시근 g를 선택한다.
- 실제 사용에서는 p는 매우 큰 소수이다.(10진수 300자리 이상)
- 주어진 문제에서는 p=13, g=2가 선택되었다.

② 송신자 A
- A는 $0 \le x \le p-1$ 범위에서 임의의 x를 선택한다. **x = 3을 선택(x는 비밀유지)**
- $a = g^x \bmod p$를 계산한다.
- $a = 2^3 \bmod 13 = 8 \bmod 13 = 8$ → **수신자 B에게 a = 8을 전송**

③ 수신자 B
- B는 $0 \le y \le p-1$ 범위에서 임의의 y를 선택한다. **y = 2를 선택(y는 비밀유지)**
- $b = g^y \bmod p$를 계산한다.
- $b = 2^2 \bmod 13 = 4 \bmod 13 = 4$ → **송신자 A에게 b = 4를 전송**

④ 송신자 A (**x = 3을 선택**)

$K_A = b^x \bmod p = 4^3 \bmod 13 = 64 \bmod 13 =$ **12**

⑤ 수신자 B (**y = 2를 선택**)

$K_B = a^y \bmod p = 8^2 \bmod 13 = 64 \bmod 13 =$ **12**

⑥ 결론
- A와 B가 구한 값은 같다. 즉, $K_A = K_B = 12$가 된다.
- A와 B는 서로 x, y 값을 모르면서 **동일한 값 12**를 얻게 된다.
- 값 12가 송수신자가 공유하는 비밀키(대칭키)가 된다.

정답 : ③

5. 다음에 설명한 Diffie-Hellman 키 교환 프로토콜의 동작 과정에서 공격자가 알지 못하도록 반드시 비밀로 유지해야 할 정보만을 모두 고른 것은? [2018년 국가 9급]

소수 p와 p의 원시근 g에 대하여, 사용자 A는 p보다 작은 양수 a를 선택하고, $x = g^a \bmod p$를 계산하여 x를 B에게 전달한다. 마찬가지로 사용자 B는 p보다 작은 양수 b를 선택하고, $y = g^b \bmod p$를 계산하여 y를 A에게 전달한다. 그러면 A와 B는 $g^{ab} \bmod p$를 공유하게 된다.

---

① a, b
② p, g, a, b
③ a, b, $g^{ab} \bmod p$
④ p, g, a, b, $g^{ab} \bmod p$

♤ **Diffie-Hellman 키 교환 프로토콜 – 비밀로 유지해야 할 정보**

① 먼저, 송수신자는 소수 p와 p의 원시근 g를 선택한다.
(p = 13, g = 7이 선택된 것으로 한다)
② 사용자 A
• A는 $0 \le a \le p-1$ 범위에서 임의의 a를 선택한다. **a = 3을 선택(a는 비밀유지)**
• $x = g^a \bmod p$를 계산한다.
$x = 7^3 \bmod 13 = 343 \bmod 13 = 5$ → 수신자 B에게 x = 5를 전송
③ 사용자 B
• B는 $0 \le y \le p-1$ 범위에서 임의의 b를 선택한다. **b = 2를 선택(b는 비밀유지)**
• $y = g^b \bmod p$를 계산한다.
$y = 7^2 \bmod 13 = 49 \bmod 13 = 10$ → 송신자 A에게 y = 10을 전송
④ 사용자 A : $K_A = y^a \bmod p = 10^3 \bmod 13 = 1000 \bmod 13 = 12$
⑤ 사용자 B : $K_B = x^b \bmod p = 5^2 \bmod 13 = 25 \bmod 13 = 12$
⑥ 결론
• A와 B가 구한 값은 같다. 즉, $K_A = K_B = 12$가 된다.
→ A와 B는 서로 a, b 값을 모르면서 동일한 값 12를 얻게 된다.
• 값 12가 송수신자가 공유하는 비밀키(대칭키)가 된다.
⑦ 분석 : 송수신자가 공유하는 대칭키는 $K = g^{ab} \bmod p$이다.
→ **$K = g^{ab} \bmod p = 7^{3 \cdot 2} \bmod 13 = 117649 \bmod 13 = 12$(비밀유지)**

정답 : ③

6. 사용자 A와 B가 Diffie-Hellman 키 교환 알고리즘을 이용하여 비밀키를 공유하고자 한다. A는 3을, B는 2를 각각의 개인키로 선택하고, A는 B에게 21(= 7^3 mod 23)을, B는 A에게 3(= 7^2 mod 23)을 전송한다면, A와 B가 공유하게 되는 비밀키 값은? (단, 소수 23과 그 소수의 원시근 7을 사용한다) [2015년 지방 9급]

① 4 ② 5
③ 6 ④ 7

♤ Diffie-Hellman 키 교환

① 먼저, 송수신자는 두 수 p와 g를 선택한다. p = 23, g = 7이 선택된 것으로 한다.
- p는 매우 **큰 소수**이다.(10진수 300자리 이상 되도록 한다)
- g는 Z_p^*의 원소 중에서 임의의 **원시근**을 선택하도록 한다.

② 송신자 A
- A는 0≤x≤p-1에서 임의의 x를 선택한다. 문제에서 **x = 3**을 선택**(x는 비밀유지)**
- a = g^x mod p를 계산한다.
- a = 7^3 mod 23 = 343 mod 23 = **21** → 수신자 B에게 **a = 21**을 전송

③ 수신자 B
- B는 0≤y≤p-1에서 임의의 y를 선택한다. 문제에서 **y = 2**를 선택**(y는 비밀유지)**
- b = g^y mod p를 계산한다.
- b = 7^2 mod 23 = 49 mod 23 = **3** → 송신자 A에게 **b = 3**을 전송

----------**문제에서 여기까지는 주어짐**----------

④ 송신자 A

$K_A = b^x \bmod p = 3^3 \bmod 23 = 27 \bmod 23 =$ **4**

⑤ 수신자 B

$K_B = a^y \bmod p = 21^2 \bmod 23 = 441 \bmod 23 =$ **4**

⑥ 결론
- A와 B가 구한 값은 같다. 즉, $K_A = K_B =$ **4**가 된다.
- A와 B는 서로 x, y 값을 모르면서 **동일한 값 4**를 얻게 된다.
- 값 **4**가 송수신자가 공유하는 **비밀키(대칭키)**가 된다.

정답 : ①

7. 공격자가 존재하는 공개된 채널을 통해 보안 통신을 원하는 갑과 을에만 비밀정보를 생성하는 Diffie Hellman 키 공유 방식에서 공개변수로 소수 p=11, 생성원 g=3이 주어졌다. 갑과 을의 개인키가 각각 2와 3일 때 공유하는 비밀값은? [2022년 군무원 9급]

① 4 ② 6
③ 8 ④ 10

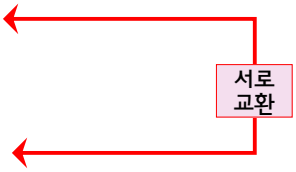
♤ Diffie Hellman 키 공유

② 통신자 **갑**은 개인키 **2**를 선택

• **갑** = 3^2 mod 11 = 9 mod 11 = **9** → **9**를 **을**에게 전송

③ 통신자 **을**은 개인키 **3**을 선택

• **을** = 3^3 mod 11 = 27 mod 11 = **5** → **5**를 **갑**에게 전송



④ 통신자 **갑** : $K_{갑} = 5^2$ mod 11 = 25 mod 11 = **3**

⑤ 통신자 **을** : $K_{을} = 9^3$ mod 11 = 729 mod 11 = **3**

⑥ 결론

• **갑**과 **을**이 구한 값은 같다. $K_{갑} = K_{을}$ = **3**이 된다.

주의!	• 주어진 문제에서 갑과 을의 **개인키**가 각각 **2**와 **3**이라 하였다. • 갑과 을의 **개인키**가 각각 **2**와 **3**이라 하여서 공개키 암호를 지칭하는 것은 아니다. • **2**와 **3**은 갑과 을이 자신만 알고 있어야 하는 **비밀값**이다.

// 이의신청

• 먼저, 정답은 ①번으로 발표되었다.
• 위의 계산 결과, 공유키는 **3**이다.
• 항목에 **3**이 없다. 정답이 없다.
• 당연, 이의신청하였다.

정답 : ①