Diffie-Hellman 기교환

- □ 1976년: Diffie와 Hellman 발표
 - ❖ 일반적으로 Diffie-Hellman(DH)키 교환으로 언급
- □ 공개키 암호의 시초
- □ 두 사용자가 안전하게 키를 교환하는 방식
- □ DH 알고리즘의 효용성은 이산 대수(discrete logarithm)계산의 어려움 에 의존
 - y=g^x (mod p) 형태에서 y를 알더라도 x를 계산하기는 불가능(어려움)

DH 알고리즘 특징

- □ 세션키를 암호화하여 전달할 필요 없음(로컬 계산)
- □ one-time random secret value 사용 (키 노출시 one traffic만 손상)
- □ 단순하고 효율적
- □ 사용자 A와 B만이 키를 계산할 수 있기 때문에 기밀성을 제공
- □ 수신자 B는 단지 사용자 A만이 이 키를 사용하여 암호화된 메시지를 생성할 수 있기 때문에 어느 정도의 인증 제공(강한 인증기능 필요)
- □ 신분 위장이나 재전송 공격을 방어 불가(Man in the Middle Attack)

DH 알고리즘 특징

□ DH 키 교환 알고리즘

전체적인 요소

9

솟수

0 < q 그리고 q의 원시근

사용자 A키 생성

개인키 X_A 선택 $X_A < q$ 공개키 Y_A 계산 $Y_A \equiv \alpha^{X_A} \mod q$

사용자 B키 생성

개인키 X_B 선택 $X_B < q$

공개키 Y_B 계산 $Y_B \equiv \alpha^{X_B} \mod q$

사용자 A에 의한 비밀키 생성

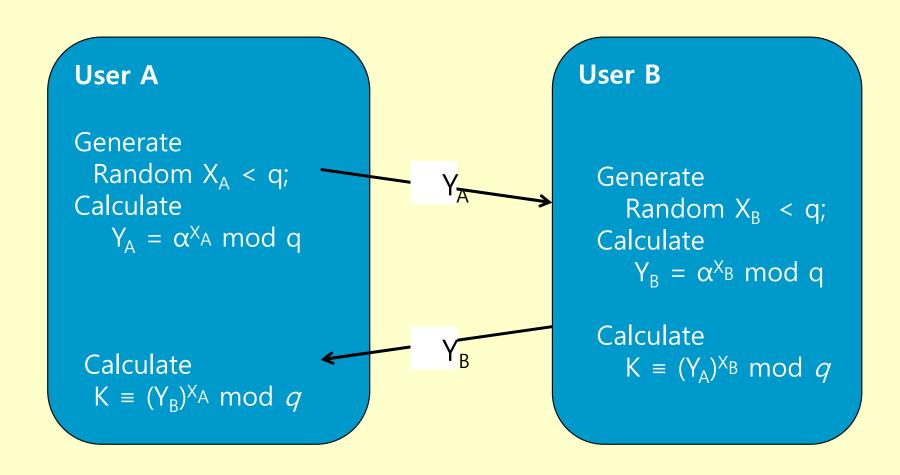
 $K \equiv (Y_R)^{X_A} \mod q$

사용자 B에 의한 비밀키 생성

 $K \equiv (Y_A)^{X_B} \mod q$

사용자 A와 B가 키 교환

□ DH 키 교환 프로토콜



사용자 A와 B가 키 교환

- lack소수 P와 원시근 정수 α 가 공개적으로 알려진 숫자
 - \triangleright A: 비밀값 X_{α} < P을 선택, $Y_{a} = \alpha^{Xa} \mod P$ 을 계산
 - ✓ A==>B: Y_a를 B에 전송
 - \triangleright B: 비밀값 $X_b < p$ 을 선택, $Y_b = \alpha^{Xb} \mod P$ 을 계산
 - ✓ B==>A: Y_b를 A에 전송.
 - ➤ A: K = Y_b(Xa) mod P 를 계산하고
 - ▶ B: K = Y_a(Xb) mod P 를 계산
- ◆ A와 B 양쪽의 K 값 계산결과는 동일하다.
- ◆ A와 B가 동일한 키 값 K를 공유

사용자 A와 B가 키 교환

$$K = Y_b^{(Xa)} \mod P$$

$$= (_{\alpha}^{Xb} \mod P)^{(Xa)} \mod P$$

$$= (_{\alpha}^{Xb})^{(Xa)} \mod P \quad (모듈로 연산규칙에 의하여)$$

$$= _{\alpha}^{XbXa} \mod P$$

$$= (_{\alpha}^{Xa})^{(Xb)} \mod P$$

$$= (_{\alpha}^{Xa} \mod P)^{(Xb)} \mod P$$

$$= Y_a^{(Xb)} \mod P = K$$

DH 키 교환 예

```
9 \alpha = 3, p = 7
```

```
A: X_a = 2 선택, Y_a = 3^2 \mod 7 = 2, Y_a 전송 Y_b 수신 후에 K = 6^2 \mod 7 = 1

B: X_b = 3 선택, Y_b = 3^3 \mod 7 = 6, Y_b 전송 Y_a 수신 후에 K = 2^3 \mod 7 = 1
```