제6장 키 관리

1. 대칭키 분배

긴 메시지 암호는 비대칭키 암호보다 속도가 빠른 대칭키 암호가 훨씬 효과적이다.
그런데, 대칭키 암호는 통신하려는 송수신자가 미리 비밀키를 공유해야 하는 단점이 있다.

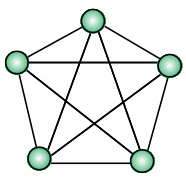
대칭키 암호에서 필요한 키의 수를 문제를 통해 살펴본다.

[예제 1] 5명의 사람들이 서로 다른 비밀통신을 하기 위해서 필요한 대칭키 수는?

[풀이 1] 두 사람이 오직 하나의 키를 사용하여 양방향 비밀통신을 한다면

- 조합(combination) 집합 = C(n, r) = C(5, 2) = (5 × 4) / 2 = 10(개)

- 이를 그래프로 표현하면 다음과 같다. - 무방향 완전그래프



- 정점수 : 비밀통신을 하려는 사람 수(5명)
- 간선수 : 비밀통신에 필요한 대칭키 수(10개)

간선수 = 대칭키 수 = n(n−1)/2 = (5 × 4) / 2 = 10(개)

[풀이 2] 만약, 두 사람이 두개의 키를 사용하여 양방향 비밀통신을 한다면

- 순열(permutation) 집합 = P(n, r) = P(5, 2) = 5 × 4 = 20(개)

[예제 2] 10,000명의 사람들이 서로 다른 비밀통신을 하기 위해서 필요한 대칭키 수는?

[풀이] 두 사람이 오직 하나의 키를 사용하여 양방향 비밀통신을 한다면

- 조합(combination) 집합
  = C(n, r)
  = C(10000, 2)
  = (10000 × 9999) / 2
  = 5000 × 9999
  = 49,995,000(개) → 약 5천만개(엄청 많다)

[분석] 대칭키를 이용한 비밀통신

① 많은 사람들이 비밀통신을 하기 위해서는 비밀키 수는 매우 많이 필요하게 된다.
→ 비밀통신하려는 개체가 증가하면, 비밀키 수는 2차함수 구조로 증가한다.

② 어떤 한 사람이 백만명과 통신한다면, 이 사람은 백만개의 비밀키가 필요하다.
→ 백만개의 비밀키를 인터넷 상에서 어떻게 교환할 것이며, 과연 안전할 것인가?

③ 백만명으로 구성된 집단이 서로 비밀통신을 한다면,
→ 이 집단에서 필요한 비밀키의 수는 약 1조개가 된다.
→ 키의 수가 많아질수록, 키 배분을 어떻게 할 것인가도 큰 문제가 된다.

[결론] 실제로, 인터넷에서는 수많은 사람들이 비밀통신을 필요로 하고 있다.

① 해서, 인터넷 상에서 비밀키 배분 및 관리를 위한 효율적인 방법이 있어야 한다.

② 우선적으로, 키의 수를 최대한 줄이기 위한 특별한 방법이 필요하다.
→ 키의 수를 줄이기 위해서는 제3의 무언가를 이용해야 한다.
→ 여기서, 제3의 무언가는 키-분배센터(KDC)이다. 뒤에서 설명한다.

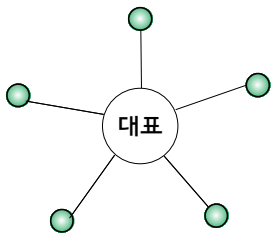
[예제 3] 어떤 그룹에 5명의 회원이 있고, 그룹의 모든 회원이 대표를 신뢰한다면, 다음과 같은 비밀 메시지 전달에 그룹에서 필요한 총 비밀키(대칭키)는 최소 몇 개인가?

> **• 회원 사이의 비밀 메시지 전달은 대표를 통해 전달한다.**
> **• 그리고, 대표는 임의 회원에게 전달받은 메시지를 다른 회원에게 전달한다.**

[풀이] 먼저, 대표와 각 회원 사이에 하나의 비밀키가 필요하다.

• 정답 : 5개의 비밀키가 필요하다.

• 이를 그림으로 표현하면 다음과 같다.



• 간선수 : 비밀통신에 필요한 비밀키 수

• 간선수 = 비밀키 수 = 5(개)

• 필요한 비밀키 수는 대표를 제외한 회원 수만큼 필요하다.
• 제3의 무언가를 이용하면, 비밀키 수를 대폭적으로 줄일 수 있다.
• 여기서, 대표가 **키-분배센터**(KDC) 개념이다. 뒤에서 설명한다.

[탐구]==========

① 만약, 회원들 사이에 직접 비밀 메시지 전달을 한다면(회원이 5명인 경우)
→ 조합 집합 = C(n, r) = C(5, 2) = (5 × 4) / 2 = 10, 10개의 비밀키가 필요

② 만약, 회원들 사이에 직접 비밀 메시지 전달에서 회원 수가 10,000명이면
→ 조합 집합 = C(n, r) = C(10000, 2) = (10000 × 9999) / 2 = **49,995,000**(개)
→ 필요한 비밀키 수는 엄청나게 증가한다.(n^2)
→ 대칭키 암호에서 **키-분배센터**(KDC)가 필요한 이유이다.

==========

기출문제 분석

1. 현재 10명이 사용하는 암호시스템을 20명이 사용할 수 있도록 확장하려면 필요한 키의 개수도 늘어난다. 대칭키 암호시스템과 공개키 암호시스템을 채택할 때 추가로 필요한 키의 개수를 각각 구분하여 순서대로 나열한 것은? [2015년 서울 9급]

① 20개, 145개　② 20개, 155개
③ 145개, 20개　④ 155개, 20개

♤ **대칭키 암호와 공개키 암호 시스템에서 키의 개수**

대칭키 암호	• 10명일 때 필요한 대칭키 수 = n(n−1)/2 = (10 × 9) / 2 = 45(개) • 20명일 때 필요한 대칭키 수 = n(n−1)/2 = (20 × 19) / 2 = 190(개) ∴ 추가로 필요한 키의 개수 = 190 − 45 = **145(개)**
공개키 암호	• 각 사용자는 (공개키, 개인키) 한 쌍만 보유하고 있으면 된다. → n명의 사용자로 구성된 공개키 암호시스템에서는 2n개의 키가 요구된다. • 10명일 때, 네트워크 전체적으로 (공개키, 개인키) : 10쌍의 키가 요구된다. → 필요한 키의 개수 = 2 × 10 = 20(개) • 20명일 때, 네트워크 전체적으로 (공개키, 개인키) : 20쌍의 키가 요구된다. → 필요한 키의 개수 = 2 × 20 = 40(개) ∴ 추가로 필요한 키의 개수 = 40 − 20 = **20(개)**

정답 : ③

2. 공개키 암호에 대한 설명으로 옳지 않은 것은? [2014년 국가 9급]

① 공개키 인증서를 공개키 디렉터리에 저장하여 공개한다.
② 사용자가 증가할수록 필요한 비밀키의 개수가 증가하는 암호방식의 단점을 해결할 수 있다.
③ 일반적으로 대칭키 암호방식보다 암호화 속도가 느리다.
④ n명의 사용자로 구성된 시스템에서는 $\frac{n(n-1)}{2}$ 개의 키가 요구된다.

♤ **공개키 암호**

• n명의 사용자로 구성된 시스템에서는 $\frac{n(n-1)}{2}$ 개의 키가 요구된다.**(×)**
→ n명의 사용자로 구성된 공개키 암호시스템에서는 2n개의 키가 요구된다.
• 각 사용자는 (공개키, 개인키) 한 쌍만 보유하고 있으면 된다.

정답 : ④