## 14.2 Symmetric Key Distribution Using Asymmetric Encryption

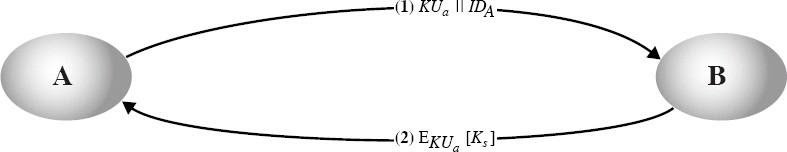
Quy trình mã hóa khóa công khai có thể được sử dụng để phân phối an toàn các khóa bí mật. Mặc dù có thể dùng mật mã khóa công khai để mã hóa thông tin nhưng vì tính kém hiệu quả, mã khóa công khai thường chậm nên người ta thường không sử dụng để mã hóa trực tiếp các khối dữ liệu kích thước lớn mà chỉ giới hạn ở các khối dữ liệu tương đối nhỏ. Do đó người ta thường phải dùng mật mã khóa bí mật để mã hóa thông tin và dùng khóa công khai mã hóa khóa bí mật cho việc phân phối.

Để đảm bảo an toàn, khóa trong mật mã khóa bí mật cần được thay đổi thường xuyên. Mỗi khóa bí mật thông thường chỉ được sử dụng trong một khoảng thời gian ngắn. Nhiều khóa bí mật thay đổi theo từng phiên làm việc (khóa phiên). Do các khóa phiên thay đổi thường xuyên nên ta cần phải có phương pháp phân phối khóa phiên một cách an toàn.

Các phương pháp cổ điển phân phối khóa gồm có:

1. Phân phối khóa phiên đơn giản
2. Phân phối khóa phiên bí mật và có xác thực
3. Cơ chế kết hợp

### 1. Simple Secret Key Distribution



Quá trình tạo và phân phối khóa đơn giản được đưa ra bởi Merkle như sau:

1. A tạo ra cặp khóa công khai tạm thời {KUA, KRA}
2. A gửi cho B khóa công khai cùng với định danh của mình KUA || IDA
3. B tạo ra khóa phiên KS, gửi nó cho A sau khi đã mã hóa nó bằng khóa công khai mà A cung cấp: EKua [KS]
4. A sử dụng khóa cá nhân của mình (KRA) giải mã để nhận được khóa phiên KS
5. A bỏ PUa, PRa và B bỏ PUa

Sau đó, A và B có thể giao tiếp với nhau một cách bí mật sử dụng mã hóa thông thường với khóa phiên KS. Lúc hoàn thành trao đổi, cả A và B loại bỏ khóa phiên KS.

Đây là quy trình đơn giản, dễ thực hiện nhưng nguy cơ bị chặn thông tin và bị mạo danh trong quá trình trao đổi là rất cao:

Trong trường hợp, nếu D có quyền kiểm soát can thiệp vào kênh liên lạc, khi đó D có thể làm hại việc giao tiếp theo cách sau mà không bị phát hiện:

1. A tạo cặp khóa {PUa, PRa} và gửi thông điệp cho B bao gồm PUa và mã định danh của A – IDA.

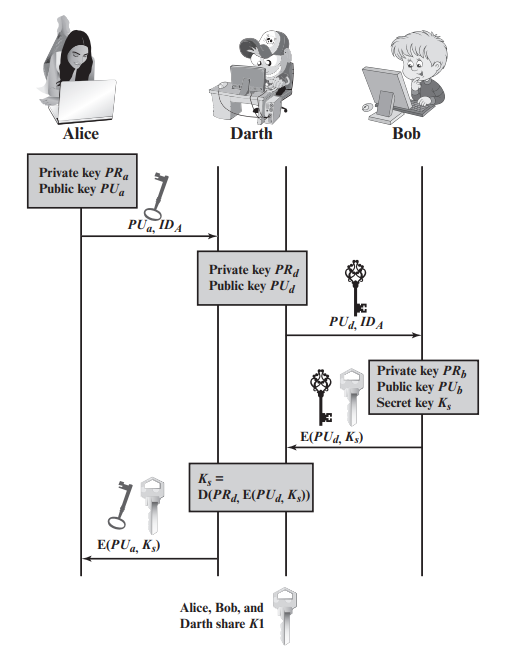
2. D chặn tin nhắn, tạo cặp khóa {PUd, PRd} và truyền PUd || IDA tới B.

3. B tạo khóa bí mật Ks và truyền E(PUd, KS).

4. D chặn tin nhắn và lấy KS bằng cách tính D(PRd, E(PUd, KS)).

5. D truyền E(PUa, KS) cho A

Kết quả là cả A và B biết KS và không hay rằng D cũng biết nó. A và B có thể trao đổi thông điệp dùng KS, D không còn can thiệp vào kênh giao tiếp mà chỉ đơn giản là nghe lén. Khi biết KS, D có thể giải mã tất cả thông điệp, cả A và B không hay biết về việc này.



### 2. Secret Key Distribution with Confidentiality and Authentication

A diagram of a physics model

Description automatically generated with medium confidence

Quy trình tạo và phân phối khóa như sau :

1. A gửi cho B thông điêp:̣ EKUb [N1 || IDA], trong đó N1 dùng để xác thực B
2. B giải mã , gắn N2 vào và gửi lại cho A: EKUa [N1 || N2], N2 – dùng để xác thực A
3. A nhận được N1 – xác thực được B. A trả lại N2 cho B: EKUb [N2]
4. B nhận được N2 – xác thực được A
5. A tao ra khóa bí mật KS , gửi nó cho B sau khi đã mã hóa hai lâǹ :

EKUb [ EKRa [KS] ]

1. B giải mã, nhận được khóa bí mật KS và sau đó cùng A sử dụng nó.

Quy trình này giống như quy trình bắt tay đã được trình bày trong phần trước. Phương pháp này tuy có phức tạp hơn so với phương pháp trên nhưng an toàn và bảo đảm được bí mật lẫn xác thực .

### 3. A Hybrid Scheme

Một cách khác để sử dụng mã hóa khóa công khai để phân phối khóa bí mật là phương pháp kết hợp được sử dụng trên các máy tính lớn của IBM [LE93]. Cơ chế này duy trì việc sử dụng trung tâm phân phối khóa (KDC) chia sẻ khóa chính bí mật với mỗi người dùng và phân phối các khóa phiên bí mật được mã hóa bằng khóa chính. Cơ sở lý luận sau đây được đưa ra để sử dụng phương pháp tiếp cận ba cấp độ này:

* Performance (Hiệu suất): Có nhiều ứng dụng, đặc biệt là các ứng dụng hướng giao dịch, trong đó khóa phiên thay đổi thường xuyên. Việc phân phối khóa phiên bằng mã hóa khóa công khai có thể làm giảm hiệu suất tổng thể của hệ thống do khối lượng tính toán tương đối cao của mã hóa và giải mã khóa công khai. Với hệ thống phân cấp ba cấp, mã hóa khóa công khai chỉ thỉnh thoảng được sử dụng để cập nhật khóa chính giữa người dùng và KDC.
* Backward compatibility (Khả năng tương thích ngược) : khả năng hoạt động của hệ thống với các phiên bản phần mềm cũ hơn. Điều này đặc biệt quan trọng trong các môi trường có nhiều thiết bị và ứng dụng khác nhau có thể không được cập nhật cùng lúc.

Việc bổ sung lớp khóa công khai cung cấp một phương tiện phân phối khóa chính an toàn, hiệu quả. Đây là một lợi thế trong cấu hình mà trong đó một KDC duy nhất phục vụ một nhóm người dùng được phân bổ rộng rãi.

Key Distribution Center (KDC) là cách tự động phân phối khóa hỗ trợ các kết nối tùy ý của các cặp người dùng. Để sử dụng KDC, chúng ta cần tối thiểu kiến trúc khóa hai cấp.

* Khóa chính (master key) được dùng để định danh người dùng
* Khóa thứ hai hay được biết đến là khóa phiên (session key) được dùng để mã hóa thông điệp giữa hai users
* Khóa phiên được mã hóa dùng khóa chính, sau đó được gửi tới clients.
* Mỗi phiên sẽ có khóa khác nhau. Theo cách này, chúng ta đã thêm 1 lớp bảo vệ, bởi vì tất cả lần truy cập được mã hóa sử dụng khóa khác nhau.
* Vì vậy, nếu attacker biết 1 khóa, khóa đó sẽ không thể giải mã tất cả thông điệp, chỉ những thông điệp được mã hóa với khóa đó.

