Rozdział 11

# Dystrybucja kluczy

W tym rozdziale opisujemy kilka metod zarządzania kluczami kryptograficznymi, w tym różne techniki dystrybucji, a także aktualizacji kluczy. Wszystkie metody omawiane w tym rozdziale obejmują zaufane centrum, które jest ostatecznie odpowiedzialne za wybór kluczy i informacje na ich temat, a potem za dystrybucję tych informacji w sieci użytkowników, którzy tego potrzebują.

## 11.1. Wprowadzenie

Stwierdziliśmy, że kryptosystemy klucza publicznego mają przewagę nad kryptosystemami z tajnym kluczem, gdyż nie jest potrzebny tajny kanał do wymiany klucza. Ale niestety większość kryptosystemów klucza publicznego (np. RSA) jest znacznie wolniejsza niż systemy z tajnym kluczem (np. AES). W praktyce więc systemy z tajnym kluczem są zwykle używane do szyfrowania „długich" komunikatów. W podrozdziale 6.1 omówiliśmy już kryptografię hybrydową, która jest często używaną metodą. Ale jest wiele innych technik, które pozwalają Alicji i Bobowi w bezpieczny sposób określić tajny klucz. Jest to nazywane *ustalaniem klucza*, co jest tematem tego i następnego rozdziału.

Omawiamy kilka podejść do problemu ustanawiania tajnych kluczy. Załóżmy, że $\mathcal{U}$ stanowi sieć złożoną z $n$ użytkowników, która nie jest bezpieczna. We wszystkich omawianych w tym rozdziale schematach mamy zaufane centrum (Trusted Authority, TA), które jest odpowiedzialne za takie sprawy, jak: weryfikowanie tożsamości użytkowników, wydawanie certyfikatów, wybór i transmisje kluczy do użytkowników itp. Jest wiele możliwych scenariuszy, obejmujących poniższe:

### Wstępna dystrybucja kluczy

W tym schemacie (*KPS – Key Predistribution Scheme*) TA „z wyprzedzeniem" dystrybuuje informacje o kluczach, w bezpieczny sposób, do każdego w sieci. Zauważmy, że bezpieczny kanał jest potrzebny w chwili dystrybucji kluczy. Potem użytkownicy sieci mogą wykorzystywać te tajne klucze do szyfrowania transmitowanych w sieci komunikatów. Tajne klucze mogą być także używane w celu uwierzytelnienia komunikatu, dzięki zastosowaniu odpowiedniego MAC. Zwykle każda para użytkowników w sieci będzie mogła w wyniku przechowywanej informacji o kluczach określić klucz (lub klucze) znane tylko im.

### Dystrybucja kluczy sesji

W dystrybucji kluczy w sieci online TA wybiera klucze sesji i przekazuje je użytkownikom sieci, gdy zostanie o to poproszone, za pośrednictwem interakcyjnego protokołu. Taki protokół nazywany jest *schematem dystrybucji klucza sesji* i jest oznaczany jako *SKDS – Session Key Distribution Scheme*. Klucze sesji są używane do szyfrowania informacji przez określony, stosunkowo krótki, czas. Klucze sesji są zaszyfrowane przez TA za pomocą wcześniej rozesłanych tajnych kluczy (przy założeniu, że każdy użytkownik sieci ma tajny klucz, którego wartość jest znana TA).

### Uzgadnianie kluczy

Uzgadnianie kluczy odnosi się do sytuacji, w której użytkownicy sieci do tworzenia klucza sesji wykorzystują interakcyjny protokół. Taki protokół nazywany jest *schematem uzgadniania kluczy* i jest oznaczany jako *KAS – Key Agreement Scheme*. Mogą to być schematy oparte na kluczu publicznym lub na kluczu tajnym i nie wymagają, aby TA było dostępne online.

Schematy wstępnej dystrybucji i dystrybucji klucza sesji są omawiane w tym rozdziale, natomiast schematy uzgadniania klucza są omawiane w rozdziale 12. Podobnie jak w rozdziale 10, bierzemy pod uwagę takie aspekty, jak: aktywni i/lub pasywni przeciwnicy, różne cele przeciwników, modele ataku oraz poziomy bezpieczeństwa.

Teraz bardziej szczegółowo porównamy i zestawimy wymienione wyżej metody ustanawiania klucza. Możemy najpierw odróżnić od siebie dystrybucję kluczy i uzgadnianie kluczy. Dystrybucja kluczy jest mechanizmem, w którym TA wybiera tajny klucz lub klucze, a następnie transmituje je do drugiej strony lub stron w zaszyfrowanej postaci. Uzgadnianie kluczy oznacza protokół, w którym dwóch (lub więcej) użytkowników sieci wspólnie ustanawia tajny klucz (zwykle klucz sesji), komunikując się kanałem publicznym. W schemacie uzgadniania klucza wartość klucza jest najczęściej określana jako funkcja wejść zapewnionych przez obie strony i tajnej informacji dwójki użytkowników. Są jednak protokoły, w których jeden użytkownik wybiera klucz (lub informacje do klucza) i wysyła drugiemu użytkownikowi w zaszyfrowanej postaci (podobnie jak to robi TA w schemacie dystrybucji klucza sesji). Ten konkretny scenariusz możemy nazwać *transportem klucza*, jeśli chcemy odróżnić go od KAS, w którym klucz zależy od obojga użytkowników.

Ważne jest odróżnienie od siebie kluczy długoterminowych od kluczy sesji. Podsumujemy teraz podstawowe cechy obu tych rodzajów kluczy.

### Klucze długoterminowe

Użytkownicy (lub pary użytkowników) mogą mieć *klucze długoterminowe* (*Long-Lived keys*, *LL-keys*), które mogą być wstępnie obliczane w razie potrzeby w sposób nieinterakcyjny na podstawie bezpiecznie przechowywanej tajnej informacji. Kluczami długoterminowymi, dalej nazywanymi kluczami LL, mogą być tajne klucze znane parze użytkowników lub, alternatywnie, użytkownikowi i TA. Z drugiej strony mogą to być prywatne klucze odpowiadające kluczowi publicznemu, przechowywanemu w certyfikatach użytkowników.