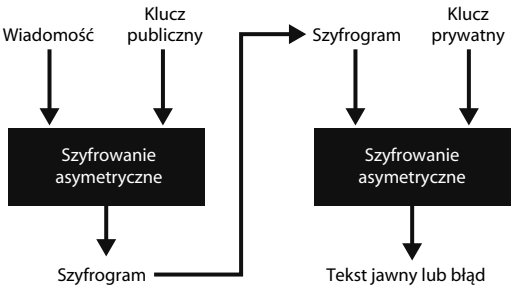


Rysunek 6.3. Szyfrowanie asymetryczne pozwala na zaszyfrowanie wiadomości (tekstu jawnego) za pomocą klucza publicznego odbiorcy. Odbiorca może następnie skorzystać z innego algorytmu, by odszyfrować zaszyfrowaną wiadomość (szyfrogram), używając do tego celu klucza prywatnego powiązanego z użytym uprzednio kluczem publicznym

Zauważmy, że jak dotąd nic nie mówiliśmy o uwierzytelnianiu. Rozważmy obie strony połączenia.

- Szyfrujemy za pomocą klucza publicznego, o którym sądzimy, że należy do Alicji.
- Alicja nie wie na pewno, kto przesłał tę wiadomość.

Na razie wyobrazimy sobie, że otrzymaliśmy klucz publiczny Alicji w rzeczywiście bezpieczny sposób. W rozdziale 7, poświęconym podpisom cyfrowym, dowiemy się, w jaki sposób rzeczywiste protokoły rozwiązują w praktyce ten problem bootstrappingu. W rozdziale 7 dowiemy sie też, jak w sposób kryptograficzny możemy zakomunikować Alicji, kim naprawdę jesteśmy. Uwaga, spoiler! – będziemy podpisywać swoje wiadomości!

Przejdźmy teraz do kolejnego podrozdziału, w którym, w której dowiemy się, jak szyfrowanie asymetryczne jest wykorzystywane w praktyce (a także dlaczego w praktyce rzadko jest wykorzystywane w bezpośredni sposób).

6.2. Szyfrowanie asymetryczne i szyfrowanie hybrydowe w praktyce

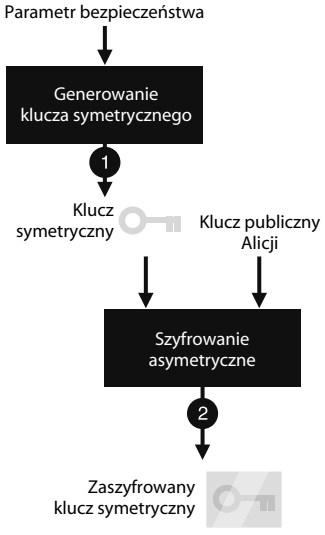
Moglibyśmy pomyśleć, że szyfrowanie asymetryczne prawdopodobnie wystarczy, by rozpocząć szyfrowanie naszych wiadomości. W rzeczywistości szyfrowanie asymetryczne jest dość ograniczone z uwagi na restrykcje dotyczące długości wiadomości, jakie może szyfrować. Szybkość asymetrycznego szyfrowania i asymetrycznej deszyfracji również jest niska w porównaniu do szyfrowania symetrycznego. Jest tak, ponieważ konstrukcje asymetryczne – w przeciwieństwie do prymitywów symetrycznych, które często po prostu manipulują bitami – implementują działania matematyczne.

W tym podrozdziale poznamy te ograniczenia, dowiemy się, do czego w praktyce stosowane jest szyfrowanie asymetryczne, a wreszcie w jaki sposób kryptografia przezwycięża istniejące przeszkody. Podrozdział ten jest podzielony na dwie części odpowiadające dwóm najważniejszym przypadkom użycia szyfrowania asymetrycznego.

- *Wymiana kluczy* – jak zobaczymy, dokonywanie wymiany klucza (lub jego uzgadniania) za pomocą prymitywu szyfrowania asymetrycznego jest całkiem naturalne.
- *Szyfrowanie hybrydowe* – jak zobaczymy, przypadki użycia są w wypadku szyfrowania asymetrycznego dość ograniczone z powodu maksymalnego rozmiaru tego, co możemy zaszyfrować. Aby szyfrować większe wiadomości, poznamy bardziej użyteczny prymityw nazywany szyfrowaniem hybrydowym.

6.2.1. Wymiany klucza i kapsułkowanie klucza

Okazuje się, że szyfrowanie asymetryczne może być używane w celu dokonania wymiany klucza – tego samego rodzaju jak ta, którą znamy z rozdziału 5! Aby to zrobić, możemy zacząć od wygenerowania klucza symetrycznego i zaszyfrowania go za pomocą klucza publicznego Alicji – operacja, którą nazywamy *kapsułkowaniem klucza* – tak jak to ilustruje rysunek 6.4.



Rysunek 6.4. Aby wykorzystać szyfrowanie asymetryczne jako prymityw wymiany klucza, (1) generujemy klucz symetryczny, a następnie (2) szyfrujemy go za pomocą klucza publicznego Alicji

Potem możemy przesłać szyfrogram do Alicji, która będzie go mogła odszyfrować i poznać klucz symetryczny. W rezultacie będziemy mieli wspólny sekret! Rysunek 6.5. przedstawia cały ten proces.

Szyfrowania asymetrycznego w celu wymiany klucza dokonuje się zwykle przy użyciu algorytmu zwanego RSA (od nazwisk jego twórców: Rivesta, Shamira i Adlemana). Jest ono wykorzystywane w wielu protokołach internetowych. Współcześnie RSA często nie jest preferowanym sposobem dokonywania wymiany klucza, a jego popularność zmniejsza się coraz bardziej i bardziej na rzecz algorytmu Diffiego-Hellmana w przestrzeni krzywych eliptycznych (ECDH). Jest tak przede wszystkim z powodów historycznych (w implementacjach i normach RSA znaleziono wiele luk) oraz atrakcyjności mniejszych rozmiarów parametrów oferowanych przez ECDH.