Janusz Stokłosa

Podpis elektroniczny

Podpis cyfrowy, nazwany przez prawników podpisem elektronicznym, wykonujemy za pomocą technik kryptograficznych. Podpis cyfrowy jest ciągiem bitów zależnym od podpisywanej wiadomości i od osoby, która podpisuje dokument. Powinien charakteryzować się co najmniej taką samą siłą i skutecznością jak podpis odręczny. Algorytmy podpisu cyfrowego projektuje się w oparciu o wybrany szyfr, stanowiący podstawę utworzenia tzw. asymetrycznego systemu kryptograficznego. W systemie takim z każdym użytkownikiem jest związana para kluczy: klucz do podpisywania wiadomości i klucz do weryfikacji podpisu. Klucz do podpisywania wiadomości jest tajny, znany tylko danej osobie, natomiast klucz do weryfikacji podpisu jest publicznie dostępny (być może dostępny w ograniczonym zakresie, np. w danej instytucji czy firmie). Podpisem wiadomości jest przekształcona kryptograficznie, za pomocą klucza tajnego, wiadomość. Weryfikacji podpisu dokonuje się przekształcając go za pomocą klucza publicznego.

W praktyce przy podpisywaniu cyfrowym korzysta się także z tzw. kryptograficznej funkcji skrótu, która przekształca wiadomość o dowolnej długości w wiadomość o niewielkiej ustalonej długości, zwanej skrótem. Funkcja ta ma tę cechę, że jest obliczeniowo trudne (w praktyce niemożliwe) znalezienie dwóch różnych wiadomości dających taki sam skrót.

Przed wykonaniem podpisu cyfrowego należy uzgodnić algorytm podpisywania (np. RSA, Rabina, El_Gamala, czy jeszcze inny) i używaną funkcję skrótu (np. MD-5, SHA-1, RIPEMD-160). Dla danej wiadomości *m* jej podpis wykonuje się w taki sposób, że najpierw oblicza się skrót *H* tej wiadomości, skrót *H* przekształca się za pomocą uzgodnionego algorytmu podpisu stosując tajny klucz kryptograficzny, w wyniku czego uzyskuje się podpis *s*.

Weryfikacja podpisu polega na odebraniu pary *(m, s)*, tj. wiadomości *m* i podpisu *s* tej wiadomości, i z jednej strony na:

(1) przekształceniu tego podpisu za pomocą algorytmu weryfikującego podpis, z wykorzystaniem klucza publicznego nadawcy wiadomości; w rezultacie weryfikacji podpisu wyznaczana jest wartość skrótu obliczonego przy podpisywaniu,

(2) obliczeniu skrótu otrzymanej wiadomości *m* i porównaniu wyniku z wartością skrótu wyznaczonego w p. (1).

Gdy się okaże, że obydwa skróty są takie same, to weryfikacja podpisu wypada pozytywnie i mamy pewność, że wiadomość *m* nie została zmieniona od momentu jej podpisania do chwili weryfikacji podpisu. Jeśli weryfikacja będzie negatywna, to wyciągniemy wniosek, że podpis jest fałszywy lub, że w trakcie przesyłania wiadomość została zmieniona.

Podpis cyfrowy jest ciągiem bitów. Może to być ciąg o długości np. 512 bitów lub większej. Zależny jest od wybranych algorytmów kryptograficznych (np. RSA, MD-5), klucza prywatnego i samej wiadomości m. Jeśli dla zwięzłości zapisu przyjąć, że ciągowi 0000 odpowiada cyfra 0, ciągowi 0001 – cyfra 2, ciągowi 0010 – cyfra 3,..., ciągowi 1001 – cyfra 9, ciągowi 1010 – litera a, ciągowi 1011 – litera b,..., wreszcie ciągowi 1111 – litera f, to przykładowy podpis będący ciągiem 1024-bitowym może być zapisany w zwartej formie jak niżej:

```
b7 2e dd a4 63 e5 1e 00 53 02 7a d3 67 83 0f 4a 00
36 be 7e 3f 53 53 e2 e8 ea b3 8b 21 17 38 80 18 ed
02 63 69 c8 48 ff 4b 88 b6 0d 22 6a f3 d1 0b cb e9
1c 24 0d f8 ad 67 38 d1 79 17 26 5c 23 30 3c 11 0d
e0 b6 21 ce e8 9c 0c 6b 62 70 c4 46 85 bd 2e 8b 32
cc 95 08 7b 20 38 ff 4d 8a 8e f8 88 f6 a1 7e 1d 23
26 1c 85 00 c1 7d 34 b8 8b 3c b2 5e d3 bb 73 a3 9f
77 9d 36 bb 27 ac af 4f 98
```

Zauważmy, że gdy podpisywana wiadomość ulegnie zmianie, to podpis też się zmieni (ciąg bitów podpisu cyfrowego będzie inny). Jest to sytuacja jakościowo różna od tej, z którą mamy do czynienia w przypadku podpisu odręcznego; podpis odręczny jest powtarzalny, a przynajmniej jego autentyczność może być potwierdzona przez grafologa. Nieco inaczej jest w przypadku podpisu cyfrowego. Żeby system podpisywania wiadomości mógł funkcjonować prawidłowo, należy stworzyć instytucję zaufanej strony trzeciej, której zadaniem będzie wystawianie certyfikatów poświadczających jakim kluczem publicznym należy się posługiwać przy weryfikacji podpisu wykonanego przez wskazaną osobę. W przypadku wątpliwości zawsze należy sprawdzać zapisany w certyfikacie związek pomiędzy daną osobą i jej kluczem publicznym służącym do weryfikacji złożonych przez nią podpisów cyfrowych.

Stosując podpisy cyfrowe należy zadać pytanie czy są one bezpieczne, tzn. czy nie jest możliwe podrobienie takiego podpisu. Techniki kryptograficzne dostarczają takich mechanizmów, które stosowane w odpowiedni sposób zapewniają większe bezpieczeństwo niż to ma miejsce w przypadku podpisów konwencjonalnych. Takie bezpieczne mechanizmy ma na uwadze ustawodawca, gdy w ustawie o podpisie elektronicznym mówi o bezpiecznym urządzeniu służące do składania podpisu elektronicznego i bezpiecznym urządzeniu służącym do weryfikacji podpisu elektronicznego.

* Autor jest profesorem w Politechnice Poznańskiej i ekspertem w zakresie kryptografii w Polskim Komitecie Normalizacyjnym.