Technologie informacyjne
przed 4 wykładem

Andrzej Giniewicz

25.03.2025

Dziś zajmiemy się podstawami naszego bezpieczeństwa w sieci.

1 Szyfrowanie i klucze

Szyfrem lub algorytmem szyfrującym będziemy nazywali ciąg operacji matematycznych, które mają na celu zapewnienie bezpieczeństwa, autentyczności i prywatności danych. Informacje, czyli tekst lub inne dane, reprezentowane jako ciągi liczb, przekształcone przez wybrany szyfr, nazywamy zaszyfrowanymi informacjami. Proces stosowania funkcji odwrotnej do funkcji szyfrującej, nazywa się deszyfrowaniem i pozwala odczytać oryginalne informacje. Aby informacja mogła być odczytana, należy wiedzieć, za pomocą jakiej funkcji została zaszyfrowana. Próbę odgadnięcia lub wyznaczenia funkcji szyfrującej, będziemy nazywać łamaniem szyfru. Jeśli o szyfrze myślimy jak o funkcji f, odszyfrowywanie będzie funkcją f^{-1}. W przykładzie poniżej informacja x zostaje zaszyfrowana do informacji y, która zostaje ponownie odszyfrowana do informacji x

$$y = f(x), \quad x = f^{-1}(y).$$

Dobre szyfry najczęściej mają następujące cechy:

- złamanie szyfru na obecnie dostępnych superkomputerach zajmuje niepraktycznie dużo czasu, np.: tysiące lat;
- zaszyfrowane dane przypominają losowy ciąg, co utrudnia znalezienie wzorców;
- zaszyfrowane dane nie pozwalają odgadnąć technologii, w której zostały zaszyfrowane.

Użyteczność funkcji szyfrującej, która nie ma parametrów, byłaby ograniczona, ponieważ wszystkie osoby znające tę funkcję mogłyby odczytać wszystkie wiadomości zaszyfrowane za jej pomocą. W tym celu zwykle wprowadza się parametr do funkcji szyfrującej, nazywany kluczem. Istnieją dwa rodzaje kluczy. Pierwszy rodzaj to klucze symetryczne, które pozwalają zarazem zaszyfrować, jak i odszyfrować wiadomość. Każda osoba znająca klucz

i metodę szyfrowania może odszyfrować i zaszyfrować wiadomość. Jeśli k to parametr oznaczający klucz, algorytm szyfrowania wykorzystujący klucz symetryczny możemy zapisać następująco

$$y = f(x,k), \quad x = f^{-1}(y,k).$$

Oznacza to, że osoba szyfrująca zna algorytm szyfrowania f, dane x i klucz k. Na ich podstawie wylicza zaszyfrowaną wiadomość y do innej osoby. Osoba ta, jeśli zna algorytm szyfrowania f i klucz k, może wiadomość odszyfrować. Zaletą tej metody jest to, że nawet jeśli zaszyfrowane dane y i metoda szyfrowania f wpadnie w niepowołane ręce, bez klucza k wciąż nie da się odczytać wiadomości.

Drugim sposobem szyfrowania jest klucz asymetryczny. W tym przypadku klucz do szyfrowania i odszyfrowywania wiadomości jest inny. Klucz do szyfrowania wiadomości nazywamy kluczem publicznym, natomiast klucz do deszyfrowania prywatnym. Jeśli klucz publiczny oznaczymy przez k_p, natomiast prywatny przez k_a, to schemat szyfrowania wygląda następująco

$$y = f(x,k_p), \quad x = f^{-1}(y,k_a).$$

Skąd nazwy kluczy: publiczny i prywatny? Zwykle klucz publiczny jest dystrybuowany do wielu osób, aby mogły zaszyfrować wiadomość, której adresatem jest konkretna osoba. Choć zaszyfrować wiadomość może wiele osób, to odczyta ją tylko ta, która ma klucz prywatny. Dlatego ważne jest, aby klucza prywatnego nie udostępniać nikomu.

Odwrotne wykorzystanie funkcji f, w którym y jest wiadomością, którą szyfrujemy za pomocą algorytmu f^{-1} oraz klucza prywatnego k_a, nazywamy podpisem cyfrowym wiadomości y. Podpis cyfrowy może zweryfikować każda osoba, która posiada odpowiedni klucz publiczny. Podsumowanie kluczy asymetrycznych znajduje się w tabeli poniżej.

	klucz publiczny	klucz prywatny
kto ma	im więcej tym lepiej	tylko jedna osoba
szyfrowanie	pozwala coś zaszyfrować	pozwala coś odszyfrować
podpis cyfrowy	pozwala sprawdzić podpis	pozwala coś podpisać

Istnieje wiele standardów szyfrowania, zarazem symetrycznego, jak i asymetrycznego. W przypadku podpisu asymetrycznego bardzo ważnym procesem jest weryfikacja poprawności klucza publicznego. Jeśli ktoś udostępni nam klucz publiczny i uwierzymy, że należy od danej osoby, każda wiadomość podpisana przez tę osobę, będzie zweryfikowana jako prawidłowa. Co jednak się stanie, jeśli uwierzymy, że klucz do kogoś należy, a w rzeczywistości został wygenerowany przez oszusta? W Internecie są tysiące a może i setki tysięcy kluczy publicznych podpisanych imionami i nazwiskami sławnych ludzi. Skąd mamy wiedzieć, który z tysięcy dostępnych Billów Gatesów jest tym prawdziwym? W praktyce wykorzystuje się dwa sposoby na sprawdzenie autentyczności kluczy:

- za pomocą urzędów certyfikacji,
- za pomocą sieci zaufania.

Sprawdzanie kluczy za pomocą urzędów certyfikacji jest bezpieczniejsze, ale bardziej kosztowne. Jest wykorzystywane tam, gdzie autentyczność podpisu jest bardzo ważna. Jednym ze standardów certyfikacji kluczy publicznych jest X.509. Jest to popularny standard, wykorzystywany między innymi do podpisu cyfrowego dokumentów w platformie ePUAP służącej do załatwiania spraw urzędowych w Polsce z wykorzystaniem tak zwanego profilu zaufanego. Certyfikacja wymaga weryfikacji tożsamości w urzędzie lub w inny pewny sposób (na przykład poprzez bank). Jednostka weryfikująca tożsamość następnie podpisuje klucz publiczny petenta. Jeśli otrzymamy od kogoś klucz publiczny, pobieramy klucz publiczny urzędu certyfikującego, dzięki czemu możemy sprawdzić podpis urzędu umieszczony pod otrzymanym kluczem publicznym i mieć pewność, że jest to ta osoba, za którą ktoś się podaje.

Do sprawdzania podpisów w wiadomościach e-mail nie stosuje się zwykle podpisów wystawianych przez urzędy certyfikacji, ponieważ koszt utrzymania takiego systemu byłby ogromny. Najczęściej używanym standardem do podpisywania i szyfrowania wiadomości o mniejszym znaczeniu strategicznym, jest standard OpenPGP. Jest to klasyczny przykład systemu opartego na sieci zaufania. Sieć zaufania to graf, w którym wierzchołkami są klucze, natomiast krawędzie informują nas o tym, że właściciel jednego klucza potwierdza autentyczność innego klucza. Krawędzie w grafie są skierowane, co oznacza, że zaufanie nie jest relacją symetryczną. Możemy komuś ufać, ale to nie znaczy, że on ufa nam. Wyróżnia się cztery poziomy zaufania, w stosunku do właścicieli kluczy.

1. Nieznane — wtedy nie wiadomo, czy osoba posługująca się kluczem, jest tym, za kogo się podaje. Jest to wartość domyślna dla nowego klucza;
2. Brak — wiemy, że właściciel klucza czasem podpisuje niezaufany klucz;
3. Częściowe — wiemy, że właściciel klucza rozumie konsekwencje wynikające z tego, że podpisuje czyjś klucz i sprawdza klucze przy podpisywaniu;
4. Pełne — wiemy, że właściciel bardzo dobrze zna koncepcje podpisywania kluczy i ufamy mu tak samo, jak sobie.

Klucz osoby B będziemy nazywać w pełni poprawnym dla osoby A, jeśli spełniony jest jeden z 3 warunków:

1. osoba A sama podpisała klucz osoby B,
2. istnieje ścieżka długości nie więcej niż 5 w sieci zaufania pomiędzy A i B taka, że wszystkie klucze są w niej w pełni zaufane,
3. istnieją trzy ścieżki długości nie więcej niż 3 w sieci zaufania pomiędzy A i B takie, że wszystkie klucze są w niej przynajmniej częściowo zaufane.

Jeśli spełniony jest warunek 3 powyżej, ale dla mniejszej liczby ścieżek, klucz nazywamy częściowo poprawnym. Klucze publiczne wraz z podpisami dystrybuowane są na serwery kluczy, aby każdy mógł sprawdzić, czy klucz danej osoby znajduje się w tej samej sieci zaufania, co jego. Niekiedy organizowane są wydarzenia polegające na tym, że osoby chcące potwierdzić swoją tożsamość spotykają się w jakimś miejscu i podpisują swoje klucze.