10 w 2025 (22)

Tajna wymiana klucza do szyfru

Data publikacji: 13.03.2025 / Autor: Michał Topolski

Jeśli przeczytałeś artykuł o kole szyfrowym, wiesz już, jak całkiem skutecznie szyfrować wiadomości. Mogłeś jednak dostrzec drogi czytelniku, że w tak szyfrowanej komunikacji trzeba jakoś wymienić się parametrami metody, którą szyfrujecie; w przypadku omawianego tam koła szyfrowego są to takie elementy jak: budowa urządzenia, przesunięcie obręczy, czy też sekwencja odczytu symboli. Poniżej przedstawiam praktyczne metody wymiany klucza bez użycia zaawansowanych programów, korzystając jedynie z fizycznej komunikacji lub nieszyfrowanych kanałów.

Dlaczego wymiana klucza jest ważna?

W szyfrowaniu symetrycznym, takim jak szyfr Cezara, zarówno nadawca, jak i odbiorca muszą znać ten sam klucz, aby zaszyfrować i odszyfrować wiadomość. Bezpieczna wymiana tego klucza jest (hehe) kluczowa, aby uniemożliwić osobom postronnym dostęp do treści komunikacji.

Jako ciekawostkę na ten moment pozostawiam fakt istnienia szyfrów asymetrycznych, których jedną z cech jest to, że do odszyfrowywania i szyfrowania korzysta się z osobnych kluczy. Może kiedyś uda się poruszyć i ten temat.

Praktyczne metody wymiany klucza

Zanim omówię matematyczny algorytm prawdziwie bezpiecznej wymiany klucza, krótko naszkicuję parę mniej bezpiecznych, ale znacznie prostszych metod, które możemy wykorzystać. Są one bardziej praktyczne i możliwe do zaimprowizowania na szybko w realnych sytuacjach, na przykład w trakcie manewrów zastępów środowiska. Można je określić jako **intuicyjne**.

1. Bezpośrednie spotkanie

Względnie bezpiecznym sposobem przekazania klucza jest osobiste spotkanie w ustronnym miejscu bez świadków. Podczas takiego spotkania można ustalić klucz,

np. liczbę przesunięcia w szyfrze Cezara, minimalizując ryzyko przechwycenia go przez osoby trzecie. Oczywiście, taka metoda ciągnie za sobą konieczność dotarcia w to samo miejsce.

Przykład:

- **Szyfr Cezara:** Ustalacie, że kluczem będzie liczba **3**, co oznacza przesunięcie każdej litery o trzy pozycje w alfabecie.
- **Koło szyfrowe:** Ustalacie sekwencję odczytu z obręczy jako **12321**, co definiuje kolejność odczytu liter z poszczególnych obręczy koła.

2. Wykorzystanie zaufanych pośredników

Jeśli bezpośrednie spotkanie nie jest możliwe, można skorzystać z zaufanej osoby, która przekaże klucz osobiście. Ważne jest, aby pośrednik był godny zaufania i świadomy znaczenia poufności klucza. Oczywiście, przy takiej metodzie wszystko opiera się na wzajemnym zaufaniu i nie mamy możliwości zweryfikować czy klucz gdziekolwiek wyciekł. Jedyną naszą gwarancją jest „na słowie harcerki/harcerza polegaj jak na Zawiszy”.

3. Podział klucza na części

Aby zwiększyć bezpieczeństwo, klucz można podzielić na kilka części i przekazać je różnymi kanałami komunikacji. Nawet jeśli jedna z części zostanie przechwycona, to bez pozostałych fragmentów klucz pozostanie niekompletny.

Przykład:

- Dzielisz klucz **12321** na fragmenty: **12**, **32**, **1**.
- Pierwszy fragment przekazujesz osobiście, drugi wysyłasz e-mailem, a trzeci przez SMS-a.

4. Ustalenie klucza na podstawie wspólnej wiedzy

Można ustalić klucz na podstawie informacji znanych tylko Tobie i odbiorcy, np. data ważnego dla Was wydarzenia. Taka metoda jest jednak najmniej bezpieczna, jeśli osoby trzecie mogą odgadnąć tę informację.

Przykład:

- Data pierwszego spotkania: **12.03.2010**.
- Klucz: suma cyfr daty: 1+2+0+3+2+0+1+0 = **9**.

O czym warto pamiętać?

- **Unikaj przesyłania klucza tym samym kanałem, którym będziesz przesyłać zaszyfrowane wiadomości.** Zmniejsza to ryzyko przechwycenia zarówno klucza, jak i treści wiadomości.
- **Regularnie zmieniaj klucz**, aby zwiększyć bezpieczeństwo komunikacji.
- **Nie używaj oczywistych kluczy**, takich jak daty urodzin czy proste sekwencje liczb np. 12345.

Algorytm Diffiego–Hellmana

Algorytm Diffiego-Hellmana to genialny sposób na uzgodnienie wspólnego tajnego klucza między dwiema osobami, nawet jeśli komunikują się przez publiczny, niezabezpieczony kanał. Kluczowa zaleta tej metody to fakt, że osoba postronna, nawet przechwytując wymieniane dane, nie jest w stanie obliczyć końcowego klucza dzięki zastosowaniu pewnych właściwości matematycznych. Jest to zatem prawdziwe bezpieczny sposób wymiany klucza. Wyjaśnię krok po kroku, jak działa ten algorytm. Zdecydowanie przyda się do niego kalkulator.

Podstawowe pojęcia – prosto i na temat

Modulo: To po prostu nic z innego jak reszta z dzielenia. Na przykład: 10 mod 3 = 1, bo 10 dzieli się przez 3 trzy razy, a reszta to 1. Modulo jest jak liczenie na zegarze – po 12 wracamy do 1.

Pierwiastek pierwotny modulo p: To liczba, która daje różne reszty przy potęgowaniu do kolejnych potęg i dzieleniu przez p. Na przykład dla p = 7, pierwiastek pierwotny g = 3, bo 3^1 mod 7 = 3, 3^2 mod 7 = 2, 3^3 mod 7 = 6, 3^4 mod 7 = 4 itd. aż skompletujemy wszystkie dostępne reszty. Nie musisz koniecznie dokładnie tego liczyć – po prostu g to liczba ustalana z góry, która 'dobrze współpracuje’ z p.

Kroki algorytmu Diffiego-Hellmana

1. **Ustalenie wartości publicznych:**

– Alicja i Bob uzgadniają wspólne wartości:

– Liczbę p: dużą liczbę pierwszą (np. 23).

– Liczbę g: pierwiastek pierwotny modulo p (np. 5).

Te wartości mogą być publicznie znane.

2. **Generowanie kluczy prywatnych i publicznych:**

– Każda strona wybiera swój tajny klucz prywatny:

  – Alicja wybiera a.

  – Bob wybiera b.

– Następnie każda strona oblicza swój klucz publiczny:

  – Alicja: A = g^a mod p.

  – Bob: B = g^b mod p.

3. **Wymiana kluczy publicznych:**

– Alicja wysyła swój klucz publiczny A do Boba.

– Bob wysyła swój klucz publiczny B do Alicji.

4. **Obliczenie wspólnego tajnego klucza:**

– Alicja oblicza: K = B^a mod p.

– Bob oblicza: K = A^b mod p.

Obie strony uzyskują ten sam wspólny klucz K, mimo że użyły różnych kluczy prywatnych (a i b).

Przykład z liczbami i obliczeniami

Załóżmy, że p = 23 i g = 5.

– Alicja wybiera a = 6 i oblicza A = 5^6 mod 23 = 8.

– Bob wybiera b = 15 i oblicza B = 5^15 mod 23 = 19.

– Wymiana kluczy publicznych:

  – Alicja wysyła A = 8 do Boba.

  – Bob wysyła B = 19 do Alicji.

– Obliczenie wspólnego klucza:

– Alicja: K = 19^6 mod 23 = 2.

– Bob: K = 8^15 mod 23 = 2.

Wspólny klucz wynosi K = 2.

Dlaczego to działa?

Algorytm opiera się na trudności rozwiązania problemu logarytmów dyskretnych – nawet jeśli ktoś zna g, p, A, i B, odgadnięcie a lub b jest praktycznie niemożliwe dla dużych liczb.

Dla osób chcących porównać swoje obliczenia przygotowałem dokument z dokładnie rozpisanymi krokami obliczania tego przykładu.

Posłowie

Bezpieczna wymiana klucza jest fundamentem skutecznej kryptografii. Stosując powyższe metody, możesz zapewnić poufność swojej komunikacji nawet bez zaawansowanych narzędzi. Powodzenia w sprawdzaniu tych metod w praktyce!

- Opis algorytmu DH na anglojęzycznej Wikipedii

Zdjęcie w tle pochodzi z zasobów 28 Gdańskiej Drużyny Harcerzy „Wilki”.

Michał Topolski

Urodzony w Kluczborku, tam też się wychował, w pewnym momencie został harcerzem, a potem instruktorem. Obecnie kierownik Wydziału Zuchów GKHy. Zawodowo zajmuje się cyberbezpieczeństwem i szkoleniami, a w wolnych chwilach uczy też debatowania. Posiada całkiem pokaźną kolekcję piór wiecznych, lubi pisać (nie tylko piórami). Zastępca redaktora naczelnego Pojutrza.