Protokoły Kryptograficzne

Arkadiusz Ostrzyżek

Contents

Diffiego-Hellmana

Definicja

Diffy-Hellman (DH) słóży do ustalenia klucza prywatnego używając jawnych kanałów komunikacji.

Wykonanie

0. Achilles i Bachus kanałem w sposób jawny ustalają p (moc zbioru) oraz g (generator).
1. Achilles i Bachus wybierają potajemnie liczby (s). Następnie wykonują peracje g^s % p = t. Wynik tych operacji przesyłają w sposób jawny sobie nawzajem.
2. Achilles i Bachus wykonują peracje na otrzymanych liczbach, t^s % p = f.

Wyniki tych operacji dadzą im ich nowy klucz do komunikacji. Będzie on taki sam, ponieważ $g^{s1}s2$ % p = $g^{s2}s1$ % p.

Atak MITM

Atakujący zna tylko: p, g, t1, t2. Oznacza to, że nie jest w stanie wykonać finalnej operacji, ponieważ t1^t2 % p != $g^{s1}s1$ % p. Atakujący musiałby w jakiś sposób pozyskać s jednej z osób, poprzez rozwiązanie logarytmu dyskretnego, który ma wysoką złożoność czasową.

Podpis niezaprzeczalny

Definicja

Składa się je pod dokumentem w podobnym celu jak zwykły podpis, jednak tym się różni od niego że sprawdzający poprawność podpisu musi skontaktować się z jego wytwórcą celem jego sprawdzenia.

Stawiający podpis ma kontrolę nad jego sprawdzaniem i sprawdzającymi.

Cechy

Użytkownik B nie może na podstawie otrzymanych danych z powyższych kroków przekonywać postronne osoby o poprawności podpisu użytkownika A.

Każdy z pozostałych użytkowników chcących sprawdzić poprawność postawionego podpisu musi wykonać powyższe kroki protokołu osobiście, natomiast użytkownik A ma kontrolę nad tym, kto taką kontrolę podpisu chce zrealizować.

Przykład

Znana jest duża liczba pierwsza p i generator g. Achilles posiada klucz prywatny (e) i publiczny(d). Chce podpisać wiadomość m.

Podpisanie wiadomości:

Achilles generuje podpis: z = mˆe (mod p)

Weryfikacja podpisu

0. Bachus losowo wybiera a i b.
1. Bachus wybiera dwie liczby losowe a i b, obie mniejsze od p, przesyła do użytkownika A wynik działania: c = zˆa*(g^x)b (mod p)
2. Achilles oblicza xˆ-1 (mod p - 1) i przesyła do Bachusa wynik działania: d = c^x(-1) (mod p)
3. Bachus sprawdza, czy: d = mˆa*gˆb (mod p).

Poprawność działań widać po podstawieniu wszystkich działań:

((m^x)a)*((g^x)b))^x(-1) = (mˆa)(gˆb)

Protokół rzutu monetą

Definicja

Protokoły służce do ustalania (losowania) wartości niezależnej od intencji użytkowników protokołów.

Cechy

- użytkownik A musi losować jakąś wartość, zanim użytkownik B zacznie odgadywać jej wartość
- użytkownik A nie może mieć możliwości dokonania ponownego losowania po usłyszeniu orzeczenia użytkownika B
- użytkownik B nie może dowiedzieć się, co wylosował użytkownik A zanim podjął decyzję.

Przykład

Rzucanie monetą z wykorzystaniem funkcji jednokierunkowej.

1. Achilles wybiera losową liczbę x, oblicza y = f(x), gdzie f(x) jest funkcją jednokierunkową i przesyła wartość y do Bachusa.
2. Bachus odgaduje, czy x jest parzyste czy nieparzyste i przesyła swoje przypuszczenie do Achillesa

3. jeśli przypuszczenie Bachusa jest poprawne, to wynikiem jest „reszka”, jeżeli nieprawdziwe, to „orzeł”, Achilles przesyła rezultat do Bachusa
4. Bachus potwierdza, że y = f(x).

Ślepe podpisy cyfrowe

Definicja

Matematyczny sposób sprawdzenia autentyczności dokumentów i wiadomości elektronicznych. Poprawny podpis oznacza, że wiadomość pochodzi od właściwego nadawcy, który nie może zaprzeczyć faktowi jej nadania oraz że wiadomość nie została zmieniona podczas transmisji.

Cechy

- niepodrabialny
- niezaprzeczalny
- autentyczny
- zapewnia integralność dokumentu
- nie można go ponownie użyć
- może istnieć niezależnie
- rózny dla róznych dokumentów
- podpisujący **nie** zna dokumentu
- nie ma możliwości powiązania pary z wykonanym protokołem
- poprawne zakończenie protokołu, generuje zawsze pare wiadomość + cert

Przykład

Ślepe podpisy można zrealizować wykorzystując RSA.

Bachus posiada klucz jawny e, klucz prywatny d i moduł jawny n. Achilles chce by Bachus podpisał na ślepo wiadomość m.

1. Achilles wybiera losowo k z przedziału 1,n
2. Achilles zaciemnia m obliczając t = mk^e (mod n) i przesyła do Bachusa
3. Bachus podpisuje t: t^d = (m*k$^{e)}$d (mod n) i przesyła Achillesowi
4. Achilles usuwa zaciemnienie t^d poprzez obliczenie s = t^d/k (mod n)