Tytuł szkolenia: Wprowadzenie do kryptografii - kompleksowe zastosowania

Kod szkolenia: INFRA-BEZP-KRYPT-KOMPL

Wprowadzenie

Kryptografię ogólnie można podzielić na symetryczną i asymetryczną. Szyfry symetryczne, strumieniowe lub blokowe, pozwalają na szybkie szyfrowanie dużych porcji danych. W ich przypadku z klucza szyfrującego można efektywnie wyznaczyć klucz deszyfrujący, dlatego klucze muszą być wymienione w bezpieczny sposób między użytkownikami. Istnieje wiele rodzajów szyfrów symetrycznych, dobrze znanymi szyframi blokowymi są Data Encryption Standard (DES) oraz Advanced Encryption Standard (AES). Szyfry symetryczne w połączeniu z funkcjami skrótu pozwalają otrzymać kody uwierzytelniające.

Jednym z pierwszych zastosowań kryptografii asymetrycznej (lub z kluczem publicznym) podanym przez Diffiego-Hellmana w 1976 był protokół, który pozwala w tajny sposób wymienić przez niezabezpieczony kanał poufną liczbę, np. klucz do szyfru symetrycznego. Kryptografia asymetryczna pozwala zrealizować szyfrowanie z kluczem publicznym i podpisy cyfrowe (wykorzystując funkcje skrótu), gdzie występują dwa klucze publiczny i prywatny. Pierwszy z nich jest jawny dla każdego i służy do szyfrowania lub weryfikacji podpisów. Klucz prywatny jest znany tylko właścicielowi i pozwala na deszyfrowanie i podpisywanie wiadomości. Bezpieczeństwo kryptosystemów asymetrycznych oparte jest na trudności rozwiązania pewnych problemów obliczeniowych. Dokładniej z pewnej tajnej wielkości można efektywnie wyznaczyć klucz prywatny i publiczny, natomiast wyznaczenie z klucza publicznego klucza prywatnego wymaga rozwiązania problemu o dużej złożoności obliczeniowej.

Dobrze znane kryptosystemy asymetryczne to RSA oparty na trudności rozkładu dużych liczb na czynniki pierwsze oraz kryptosystemy w ciałach skończonych i na krzywych eliptycznych oparte na trudności rozwiązania problemu logarytmu dyskretnego. Stosując krzywe eliptyczne można otrzymać efektywniejsze kryptosystemy, ponieważ istnieją efektywniejsze metody łamania RSA, np. dla poziomu bezpieczeństwa 80 bitów, w przypadku krzywych eliptycznych można stosować około 8 razy krótszy klucz niż w przypadku RSA, przez co otrzymuje się znacznie efektywniejszy kryptosystem. Istotną rolę w kryptografii asymetrycznej odgrywa autentyczność klucza publicznego potwierdzana przez certyfikaty cyfrowe. Kryptografia asymetryczna jest znacznie wolniejsza od symetrycznej, dlatego w praktyce stosuje się ją głównie do podpisów cyfrowych i wymiany kluczy szybkich szyfrów symetrycznych, które wykorzystuje się do szyfrowania dużych danych. W praktyce można wykorzystać oprogramowanie kryptograficzne, np. PGP, GNU Privacy Guard (GPG), openSSL, pozwalającym m.in. na szyfrowanie wiadomości, uwierzytelnienie i podpisy cyfrowe. Kryptografia jest stosowana w protokołach internetowych TLS/SSL dających poufność, integralność i uwierzytelnienie oraz w protokole SET (Secure Electronic Transactions) bezpiecznych transakcji z użyciem kart kredytowych. Implementacja wybranych algorytmów kryptograficznych jest dostępna w bibliotekach programistycznych C, C++, Java. Kryptografia jest również dziedziną stale się rozwijającą i mającą inne zastosowania m.in. szyfrowanie homomorficzne, bezpieczne obliczenia wielostronne, elektroniczne głosowania, kryptowaluty (bitcoin).

Adresaci szkolenia

Osoby zainteresowane wykorzystaniem kryptografii, zrozumieniem działania podstawowych kryptosystemów i ich implementacji. Zajęcia są prowadzone od podstaw i nie jest wymagana żadna specjalna wiedza, chociaż użyteczna jest pewna wiedza o programowaniu. Istnieje możliwość dokładniejszego omówienia wybranych partii materiału w zależności od indywidualnych potrzeb oraz rozszerzenia szkolenia o dodatkowy materiał.

Sprawdź zakres tematyczny innych szkoleń z krytpgorafii:

1. Wprowadzenie do kryptografii - podstawowe zastosowania (3 dni)
2. Wprowadzenie do kryptografii - rozszerzone zastosowania (3 dni)

Cel szkolenia

Celem szkolenia jest m.in. elementarne przedstawienie następujących zagadnień:

- wprowadzenie podstawowych faktów i metod matematycznych wykorzystywanych w kryptografii,
- wprowadzenie podstawowych pojęć i operacji kryptograficznych, ich własności i zastosowań,
- opis standardowych kryptosystemów symetrycznych i asymetrycznych na poziomie potrzebnym do zrozumienia ich działania i implementacji,
- zastosowania wybranych programów kryptograficznych i bibliotek programistycznych,
- samodzielne ćwiczenia z implementacji wybranych algorytmów i kryptosystemów oraz wykorzystania programów kryptograficznych,
- omówienie wybranych ataków na kryptosystemy,
- wprowadzenie podstaw pozwalających na rozszerzenie wiedzy.

Czas i forma szkolenia

- 35 godzin (5 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

Plan szkolenia

1. Klasyczne szyfry i metody ich łamania: szyfry podstawieniowe i oparte na permutacjach, szyfr Vigenere, Hilla, podstawowe typy ataków ze znanym lub wybranym tekstem jawnym (szyfrogramem), kryptoanaliza częstościowa.
2. Kryptografia symetryczna: szyfry strumieniowe, one time pad, szyfry RC4, Trivium i in., generatory pseudolosowe. Szyfry blokowe DES, 3DES, AES, Blowfish i in, tryby działania szyfrów blokowych ECB, CBC, OFB, CTR, CFB, kryptoanaliza liniowa i różnicowa.
3. Funkcje skrótu: paradoks dnia urodzin, funkcje skrótu Merkle-Damgard, MD5, Secure Hash Algorithm SHA-1, SHA-2, RIPEMD, kody uwierzytelnienia wiadomości, HMAC, commitments.
4. Podstawowe fakty z teorii liczb, własności ciał skończonych i krzywych eliptycznych: rozszerzony algorytm Euklidesa, chińskie twierdzenie o resztach, twierdzenie o liczbach pierwszych, testowanie pierwszości, reprezentacja ciał skończonych, implementacja podstawowych działań w ciałach skończonych, definicja dodawania punktów na krzywych eliptycznych.
5. Kryptografia asymetryczna: kryptosystem RSA, kryptosystemy oparte na problemie logarytmu dyskretnego w ciałach skończonych i na krzywych eliptycznych, porównanie poziomów bezpieczeństwa tych kryptosystemów, wymiana kluczy Diffiego-Hellmana, szyfrowanie ElGamala, standard podpisu cyfrowego DSA i ECDSA, infrastruktura klucza publicznego, certyfikaty, protokół Kerberos.
6. Protokoły sieciowe i oprogramowanie kryptograficzne: protokoły sieciowe SSL, TLS, IPsec, Secure Electronic Transaction (SET), oprogramowanie kryptograficzne Pretty Good Privacy (PGP), GNU Privacy Guard (GnuPG), OpenSSL, wykorzystanie bibliotek programistycznych.
7. Wybrane metody łamania RSA i kryptosytemów opartych na problemie logarytmu dyskretnego: faktoryzacja metodą baz rozkładu, metoda faktoryzacji Lenstry oparta na krzywych eliptycznych, metody rho-Pollarda, indeksu, Polliga-Hellmana, atak kanałem pobocznym.
8. Protokoły kryptograficzne i inne zastosowania: zastosowania iloczynów dwuliniowych na krzywych eliptycznych w realizacji kryptografii opartej na tożsamości i tworzeniu krótkich podpisów cyfrowych, współdzielenie sekretów, szyfrowanie i podpisy progowe, protokoły zerowej wiedzy, bezpieczne obliczenia wielostronne, głosowania i aukcje elektroniczne, kryptowaluty - bitcoin.