BDAN

Bezpieczeństwo danych

Projekt: Profesjonalny algorytm kryptograficzny

Cel projektu programistycznego

- Celem tego projektu jest samodzielne zaprogramowanie algorytmu kryptograficznego w sposób profesjonalny.
- Oznacza to, że algorytm powinien zostać zapisany w formie nadającej się do wykorzystania przez innych użytkowników.
- Powinna zostać przetestowana i udokumentowana poprawność jego działania.
- Do sprawdzenia poprawności działania muszą zostać wykorzystane wektory testowe (zwykle dostarczane przez projektanta w specyfikacji algorytmu).
- Do sprawozdania powinna być załączona dokumentacja algorytmu.
- Językiem programowania może być dowolny język programowania za wyjątkiem języka C (programy w tym języku są zwykle dostępne wraz ze specyfikacją algorytmu i mogą być pomocne przy analizie działania algorytmu).

Dlaczego takie wymagania ?

- W ostatnich latach stwierdzono, że dotychczas stosowane algorytmy kryptograficzne wymagają zastąpienia przez nowe konstrukcje, które:
  - Będą opracowane na podstawie jasnych założeń projektowych
  - Będą wykorzystywać zdobycze nowoczesnej matematyki
  - Będą miału dobre cechy użytkowe, to znaczy:
    - Będą skalowalne pod względem wydajności
    - Będą opisane przez standaryzowany zestaw parametrów, tworząc rodziny algorytmów
    - Będą skalowalne pod względem mocy platformy sprzętowej
    - Będą realizowalne programistycznie i sprzętowo
- Ponadto:
  - Konstrukcje te są zaprezentowane w sposób jednolity, umożliwiający porównanie z analogicznymi konstrukcjami
  - Dostępna jest aplikacja referencyjna (**w języku C**) wraz z zestawem wektorów testowych

Konkursy tematyczne

- AES: the Advanced Encryption Standard
- eSTREAM: the ECRYPT Stream Cipher Project
- SHA-3: a Secure Hash Algorithm
- PHC: Password Hashing Competition
- CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness

AES: the Advanced Encryption Standard

- M-17, 1997.01.02: NIST announces AES competition.
- M-14, 1997.04.15: AES Evaluation Criteria/Submission Requirements
- M-9, 1997.09.12: NIST issues call for algorithms.
- M0, 1998.06.15: Deadline for submissions.
- M2, 1998.08.20: First AES Candidate Conference. NIST announces 15 AES candidates.
- M14, 1999.08.09: NIST announces its selection of 5 AES finalists.
- M28, 2000.10.02: NIST announces its selection of AES.

eSTREAM: the ECRYPT Stream Cipher Project

- M-6, 2004.10.14–15: SASC: The State of the Art of Stream Ciphers.
- M0, 2005.04.29: Deadline for cipher submissions. 34 ciphers were submitted.
- M11, 2006.03.27: eSTREAM committee announces list of 27 second-round ciphers.
- M24, 2007.04.06: eSTREAM committee announces list of 16 finalists.
- M36, 2008.04: eSTREAM committee announces portfolio of 8 ciphers.
- M41, 2008.09: eSTREAM committee announces revised portfolio of 7 ciphers.

SHA-3: a Secure Hash Algorithm

- M-21, 2007.01.23: NIST announces SHA-3 competition and draft requirements.
- M-12, 2007.10.29: NIST publishes call for submissions, including final requirements.
- M0, 2008.10.31: Deadline for submissions.
- M2, 2008.12.10: NIST announces selection of 51 first-round candidates.
- M9, 2009.07.24: NIST announces selection of 14 second-round candidates.
- M26, 2010.12.09: NIST announces selection of 5 finalists.
- M48, 2012.10.02: NIST announces selection of SHA-3.

PHC: Password Hashing Competition

- In Q1 2013: the call for submissions
- March 31, 2014: received 24 submissions
- December 2014: 9 finalists
- July 2015: announced **Argon2** as a winner
- special recognition to four of the finalists:
  - Catena, for its agile framework approach and side-channel resistance
  - Lyra2, for its elegant sponge-based design, and alternative approach to side-channel resistance
  - Makwa, for its unique delegation feature and its factoring-based security
  - yescrypt, for its rich feature set and easy upgrade path from scrypt

CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness

- M-20, 2012.07.05–06: DIAC: Directions in Authenticated Ciphers. Stockholm.
- M-14, 2013.01.15: Competition announced.
- M0, 2014.03.15: Deadline for first-round submissions.
- M16, 2015.07.07: Announcement of second-round candidates.
- M29, 2016.08.15: Announcement of third-round candidates.
- M48, 2018.03.05: Announcement of finalists.
- M59: 2019.02.20: Announcement of final portfolio. :

Komitety ewaluacyjne

- CRYPTREC: Cryptography Research and Evaluation Committee
- NESSIE: New European Schemes for Signatures, Integrity, and Encryption

CRYPTREC: Cryptography Research and Evaluation Committee (Japonia)

- W efekcie działania wskazano algorytmy nie we wszystkich klasach. Wiele wskazań pokrywa się z rekomendacjami innych organizacji. Zawiera tez kilka oryginalnych rozwiązań japońskich, np.
- 128-bit block ciphers
  - Camellia: Nippon Telegraph and Telephone, Mitsubishi Electric
- Key exchange
  - PSEC-KEM: Nippon Telegraph and Telephone
- 64-bit block ciphers
  - CIPHERUNICORN-E: NEC
  - Hierocrypt-L1: Toshiba
  - MISTY1: Mitsubishi Electric
- 128-bit block ciphers
  - CIPHERUNICORN-A: NEC
  - CLEFIA: Sony
  - Hierocrypt-3: Toshiba
  - SC2000: Fujitsu
- Stream ciphers
  - MUGI: Hitachi
  - Enocoro-128v2: Hitachi
  - MULTI-S01: Hitachi

NESSIE: New European Schemes for Signatures, Integrity, and Encryption (Europa)

- Block ciphers
  - MISTY1: Mitsubishi Electric
  - Camellia: Nippon Telegraph and Telephone and Mitsubishi Electric
  - SHACAL-2: Gemplus
  - AES*: (Advanced Encryption Standard) (NIST, FIPS Pub 197) (aka Rijndael)
- Public-key encryption
  - ACE Encrypt#: IBM Zurich Research Laboratory
  - PSEC-KEM: Nippon Telegraph and Telephone Corp
  - RSA-KEM*: RSA key exchange mechanism (draft of ISO/IEC 18033-2)
- MAC algorithms and cryptographic hash functions
  - Two-Track-MAC: Katholieke Universiteit Leuven and debis AG
  - UMAC: Intel Corp, Univ. of Nevada at Reno, IBM Research Laboratory, Technion Institute, and Univ. of California at Davis
  - CBC-MAC*: (ISO/IEC 9797-1);
  - EMAC: Berendschot et al.
  - HMAC*: (ISO/IEC 9797-1);
  - WHIRLPOOL: Scopus Tecnologia S.A. and K.U.Leuven
  - SHA-256*, SHA-384* and SHA-512*: NSA, (US FIPS 180-2)
- Digital signature algorithms
  - ECDSA: Certicom Corp
  - RSA-PSS: RSA Laboratories
  - SFLASH: Schlumberger Corp
- Identification schemes
  - GPS-auth: Ecole Normale Supérieure, France Télécom, and La Poste:

Cel projektu programistycznego, dokładniej

- Zaprogramowanie w języku programowania, innym niż C, algorytmu należącego do jednej z klas:
  - Szyfr blokowy
  - Szyfr strumieniowy
  - Funkcja skrótu
  - Metoda zabezpieczenia hasła
  - Algorytm uwierzytelnionego szyfrowania
- Trzeba wybrać jedna z powyższych klas i zgłosić swój wybór do prowadzącego projekt.
- Prowadzący prześle dokumentacje algorytmu do zaprogramowania należącego do wskazanej klasy.

Szyfr blokowy

- Na konkurs AES zgłoszono wiele znakomitych algorytmów.
- Wygrał Rijndael i został standardem NIST.
- Niektóre z pozostałych algorytmów stosowane są jako standardy narodowe lub firmowe.
- Jest wśród nich wiele ciekawych konstrukcji – pole do popisu dla programistów.
- Lars R. Knudsen, Matthew J.B. Robshaw, The Block Cipher Companion, Springer-Verlag Berlin Heidelberg 2011.

Szyfr strumieniowy

- Zgłoszenia do eSTREAM były oczekiwane w ramach jednego (lub obu) z następujących dwóch profili:
  - Profil 1: Szyfruj strumienie dla aplikacji o wysokiej przepustowości.
    - Musi obsługiwać klucz 128-bitowy.
    - Musi obsługiwać 64-bitową IV i 128-bitową IV.
  - Profil 2: Szyfruj strumienie dla aplikacji sprzętowych o bardzo ograniczonych zasobach.
    - Musi obsługiwać klucz 80-bitowy.
    - Musi obsługiwać 32-bitowy IV i 64-bitowy IV.
- Przedstawiono ciekawe konstrukcje oparte na LFSR i innych typach rejestrów
- Matthew Robshaw, Olivier Billet (Eds.), New Stream Cipher Designs. The eSTREAM Finalists, Springer-Verlag Berlin Heidelberg 2008.

Funkcja skrótu

- Przedstawiono różnorodne konstrukcje realizujące skróty o długościach:
  - SHA-224,
  - SHA-256,
  - SHA-384,
  - SHA-512.
- Propozycje oparte są na różnorodnych schematach, nie tylko na tradycyjnych schemacie M-D czy też zwycięskim sponge.

Metoda zabezpieczenia hasła

- Skracanie haseł (password hashing) stosowane jest w wielu aplikacjach, od przechowywania poświadczeń usług internetowych po systemy uwierzytelniania mobilnego i stacjonarnego lub szyfrowania dysku.
- Nie było ustalonego standardu, który byłby w stanie zaspokoić potrzeby nowoczesnych aplikacji i najlepiej chronić hasła przed atakującymi.
- Rozwiązaniu tego problemu służył konkurs PHC).
- Dał w rezultacie kilka interesujących rozwiązań, wartych oprogramowania, np.
  - Argon2;
  - Catena;
  - Lyra2;
  - Makwa;
  - Yescryp;
  - Kilkadziesiąt innych, do wyboru.

Algorytm uwierzytelnionego szyfrowania

- Uwierzytelnione szyfrowanie może być zrealizowane za pomocą odpowiedniego tryby pracy szyfru blokowego.
- Może też być efektem specjalnie zaprogramowanego algorytmu, na przykład zgłoszonego na konkurs CAESAR.
- Do wyboru jest jeden z prawie 60 kandydatów z tego konkursu lub tryb pracy szyfru blokowego z oferty NIST.

Przygotowanie do realizacji zadań

- Wybór zadania
  - Wybór języka programowania.
  - Wybór kategorii algorytmu do zrealizowania.
  - Zgłoszenie propozycji kategorii do prowadzącego projekt.
  - Przesłanie propozycji algorytmu do zrealizowania do zespołu (dokumentacja algorytmu).
  - Negocjacja wyboru algorytmu i przyjęcie zadania do realizacji.
- Realizacja zadania
  - Zaprogramowanie i przetestowanie aplikacji w wybranym języku programowania.
  - Sporządzenie dokumentacji zrealizowanego zadania.
- Prezentacja zadania
  - Przygotowanie prezentacji zrealizowanego zadania
  - Przedstawienie prezentacji (w formie wynikającej z rozwoju sytuacji epidemicznej).

Ocenianie

- Zaliczenie tego laboratorium odbywa się w formie przesłania raportu do prowadzącego i przedstawienia prezentacji.
- Każdy dwuosobowy zespół prezentuje wykonanie zadań w przydzielonym języku programowania
  - Oprócz prezentacji wykonania samych zadań należy przedstawić konstrukcje zrealizowanego algorytmu.
- Maksymalny czas prezentacji to 10 minut.
- Kody z wykonanymi zadaniami należy dostarczyć odpowiedniemu prowadzącemu do końca dnia zaliczenia prezentacji: 2VI i 5VI.
- **Bonus:** Wybór innego języka niż java jest premiowany dodatkowymi punktami (maks. 5) w zależności od jakości wykonania (kod + dokumentacja).

Profesjonalny algorytm kryptograficzny

Projekt BDAN, Zadanie 3