Bezpieczeństwo komputerowe

semestr letni 2023/24

Lista nr 4

(laboratorium)

Terminy oddania: przed 11.05.2024

Zadanie 1. Bezpieczeństwo RSA (15 pkt). Napisz w wybranym języku programowania program do generowania pary kluczy RSA na podstawie podanych liczb pierwszych p oraz q. Za pomocą tego progarmu zasymuluj sytuację współdzielenia tego samego modułu n przez dwie różne ososby. W tym celu wygeruj dwie różne pary kluczy $(sk_A, pk_A) = ((n, d_A), (n, e_A))$ oraz $(sk_B, pk_B) = ((n, d_B), (n, e_B))$ dla tych samych parametrów wejściowych, czyli dwóch różnych dużych liczb pierwszych p i q (pamiętaj o sprawdzaniu pierwszości paramerów wejściowych p oraz q). Następnie zakładając, że masz dostęp tylko do pary kluczy (sk_A, pk_A) oraz klucza publicznego pk_B, zaimplementuj algorytm (podany na wykładzie) pozwalający wyliczyć klucz prywatny sk_B.

Zadanie 2. Podpisy e-dowód (10 pkt). Zadanie składa się z kilku etapów:

1. Jeżeli jeszcze nie posiadasz, to załóż profil zaufany[1] https://pz.gov.pl/pz/index (uwaga: jeżeli ze względów formalnych nie możesz tego zrobić, to przejdź do wersji B tego zadania).
2. Poszukaj informacji na temat tego, na czym polega usługa **podpisu zaufanego**. Kiedy i kto może z niej skorzystać?
3. Przygotuj dokument testowy w wybranym przez Ciebie formacie i skorzystaj z usługi składania podpisu zaufanego za pomocą serwisu Rzeczypospolitej Polskiej dostępnej pod adresem https://moj.gov.pl/uslugi/signer/upload?xFormsAppName=SIGNER (znajdziesz tam listę obsługiwanych formatów dokumentów). Serwis ten umożliwia również uproszczoną weryfikację złożonego podpisu zaufanego. Zwróć uwagę na format, jaki może mieć podpis zaufany - XAdES lub PAdES. Czym się charakteryzują?

[1] Profil zaufany jest bezpośrednio powiązany z Elektroniczną Platformą Usług Administracji Publicznej (ePUAP) i z jednej strony umożliwia do niej dostęp (usługa uwierzytelniania), z drugiej można go wykorzystać do podpisywania dowolnego dokumentu elektronicznego podpisem zaufanym, będącym integralną częścią profilu zaufanego

4. Wykorzystaj System Automatycznej Weryfikacji Podpisu Elektronicznego (SAWPE) firmy Madkom SA[2] (https://weryfikacjapodpisu.pl) do weryfikacji złożonego przez Ciebie podpisu zaufanego. Znajdź informacje na temat certyfikatu podpisującego:
   - na kogo i przez kogo został wystawiony?
   - czy znajduje się na liście CRL (i czym owa lista jest)?
   - jak wygląda cała ścieżka certyfikacji?
5. Zmień cokolwiek nieistotnego w podpisanym dokumencie, np. dostaw kropkę (nie zmieniając wartości podpisu). Przeprowadź ponownie proces weryfikacji podpisu. Co się zmieniło?
6. Pobierz przykładowy dokument podpisany **podpisem osobistym** z e-dowodu z wykorzystaniem formatu PadES: https://cs.pwr.edu.pl/lauks/sec/sec-lab4-testowy-osobisty-eDOApp.pdf. Zweryfikuj go przy użyciu https://weryfikacjapodpisu.pl. Co oznacza, że wystawca certyfikatu jest niezaufany?
7. Jakie są różnice pomiędzy podpisem zaufanym, osobistym a kwalifikowanym dostępnymi dla e-dowodu i e-PUAP?

Wersja B zadania 2:
Pod adresem https://cs.pwr.edu.pl/lauks/sec/sec-lab4-zaufany.zip znajdziesz przykładowy plik tekstowy – `testowy.txt`, jego podpisaną wersję w formacie XAdES – `testowy.txt.xml`, wersję podpisaną ze zmodyfikowaną wiadomością – `testowy2.txt.xml`. Korzystając z https://www.base64decode.org/ sprawdź treści podpisanych wiadomości w przypadku obydwu podpisów a następnie wykonaj pozostałe kroki zadania 1, te które nie wymagają dostępu do profilu zaufanego.

[2]Firma Madkom SA jest dostawcą niekwalifikowanych usług zaufania, wpisanym do Rejestru Dostawców Usług Zaufania prowadzonego przez Narodowy Bank Polski (https://www.nccert.pl/uslugiNK.htm). Zasady świadczenia usługi są regulowane przez Politykę świadczenia usługi https://weryfikacjapodpisu.pl/policy