Kryptografia i bezpieczeństwo

Laboratorium - lista nr 8, do 8 I

Zadanie 1 (5 pkt) Zabezpiecz "stronę bankową"[1] przed atakami:

1. SQL-injection (zapoznaj się z `https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet`),
2. XSS (`https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet`),
3. XSRF (`https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Preventi` `Cheat_Sheet`).

Zadanie 2 (5 pkt) Zaimplementuj "książkowe" szyfrowanie i podpisywanie RSA (do generowania liczb pierwszych możesz wykorzystać wbudowane algorytmy): generowanie klucza, szyfrowanie, deszyfrowanie oraz generowanie klucza, podpisywanie, weryfikację podpisu.

Implementacja musi wykorzystywać dwie wersje potęgowania: jedną tradycyjną, drugą wykorzystującą Chińskie Twierdzenie o Resztach. Potęgowanie zaimplemntuj samodzielnie – wykorzystaj szybkie potęgowanie (będzie potrzebne na kolejnych listach).

Musisz znać złożoność obliczeniową każdego z wykorzystywanych algorytmów (mnożenie, dodawanie, potęgowanie, algorytm Euklidesa, CRT, ...).

Przydatną funkcją umożliwiającą dokładny pomiar liczby cykli jest *rdtsc*.

[1] jeżeli zachodzi potrzeba – w szczególności, gdy została stworzona w php. Jeżeli została stworzona za pomocą języka/frameworka, który sam wymusza takie zabezpieczenia, to musisz umieć wyjaśnić w jaki sposób jest to osiągane.