**Sprawozdanie nr 6**

**z przedmiotu Wybrane Elementy Kryptologii**

1. **Zagadnienie**

Podpis cyfrowy.

1. **Cel**

Zajęcia laboratoryjne realizowane z wykorzystaniem programu CryptTool 2.1 mające na celu zapoznanie się z podstawowymi schematami podpisu cyfrowego: RSA, ElGamala i DSA i ich bezpieczeństwem.

1. **Zadania do realizacji w sprawozdaniu**
2. Podpis cyfrowy: schemat RSA
3. Korzystając z modeli utworzonych na poprzednich laboratoriach opracuj model realizujący generowanie i weryfikację podpisu cyfrowego schematem RSA. Przy pomocy opracowanego modelu wygeneruj klucz publiczny i prywatny o długości co najmniej 1024 bitów i korzystając z jednej z tych dwóch funkcji skrótu (SHA-2 albo SHA-3) wyznacz podpis dokumentu złożonego z własnego imienia i nazwiska (i ewentualnie dodatkowych danych). Następnie zweryfikuj uzyskany podpis. W sprawozdaniu zamieść poprawnie opisane wszystkie wartości: p, q, n, ϕ, e, d oraz podpisywany dokument, jego skrót oraz wygenerowany podpis.
4. Dla danych, zamieszczonych w załączonym do tego zadania pliku, w wierszu odpowiadającym Twojemu numerowi w grupie, korzystając z opracowanego modelu, zweryfikuj podany podpis. W przypadku negatywnej weryfikacji podaj jej przyczynę. Po wyznaczeniu wszystkich wymaganych wartości uzupełnij tabelkę i zamieść ją w sprawozdaniu.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Lp. | n | e | Skrót h(M) | Podpis s | Ważność podpisu (tak/nie) | Przyczyna |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. Podpis cyfrowy: schemat ElGamala
2. Korzystając z modeli i danych (p i g) utworzonych na poprzednich laboratoriach opracuj model realizujący generowanie i weryfikację podpisu cyfrowego schematem ElGamala. Przy pomocy opracowanego modelu wygeneruj klucz publiczny i prywatny i korzystając z jednej z dwóch funkcji skrótu (SHA-2 albo SHA-3) wyznacz podpis dokumentu złożonego z własnego imienia i nazwiska (i ewentualnie dodatkowych danych). Następnie zweryfikuj uzyskany podpis. Generowanie i weryfikację powtórz dla dwóch różnych wartości parametru k. W sprawozdaniu zamieść poprawnie opisane wszystkie wartości: p, g, x, y, k oraz podpisywany dokument, jego skrót oraz wygenerowany podpis.
3. Dla danych, zamieszczonych w załączonym do tego zadania pliku, w wierszu odpowiadającym Twojemu numerowi w grupie, korzystając z opracowanego modelu, zweryfikuj podany podpis. W przypadku negatywnej weryfikacji podaj jej przyczynę. Po wyznaczeniu wszystkich wymaganych wartości uzupełnij tabelkę i zamieść ją w sprawozdaniu.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Lp. | p | g | y | Skrót h(M) | Podpis (r, s) | Ważność podpisu (tak/nie) | Przyczyna |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

1. Podpis cyfrowy DSA
2. Korzystając z poprzednich zadań opracuj model realizujący generowanie i weryfikację podpisu cyfrowego algorytmem DSA. Przy pomocy opracowanego modelu wygeneruj klucz publiczny i prywatny i korzystając z jednej z dwóch funkcji skrótu (SHA-2 albo SHA-3) wyznacz podpis dokumentu złożonego z własnego imienia i nazwiska (i ewentualnie dodatkowych danych). Następnie zweryfikuj uzyskany podpis. Generowanie i weryfikację powtórz dla dwóch różnych wartości parametru k. W sprawozdaniu zamieść poprawnie opisane wszystkie wartości: p, q, g, x, y, k oraz podpisywany dokument, jego skrót oraz wygenerowany podpis.
3. Dla danych, zamieszczonych w załączonym do tego zadania pliku, w wierszu odpowiadającym Twojemu numerowi w grupie, korzystając z opracowanego modelu, zweryfikuj podany podpis. W przypadku negatywnej weryfikacji podaj jej przyczynę. Po wyznaczeniu wszystkich wymaganych wartości uzupełnij tabelkę i zamieść ją w sprawozdaniu.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lp. | p | q | b | c | Skrót h(M) | Podpis (r, s) | Ważność podpisu (tak/nie) | Przyczyna |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Wyniki**

W celu zaliczenia zagadnienia nr 6 należy oddać:

1. Pliki projektowe wykonane w CryptTool dla każdego podpunktu.
2. Sprawozdanie z opisem działania każdego opracowanego modelu wraz z zrzutami ekranu wykonanych modeli.
3. Dla każdej operacji generowania podpisu cyfrowego w sprawozdaniu należy umieścić: wiadomość, jej skrót, klucz prywatny i uzyskany podpis, a dla operacji weryfikacji: podpis, wiadomość i jej skrót, klucz publiczny i wynik weryfikacji