Bezpieczeństwo Systemów i Usług Informatycznych

Laboratorium 4 - Rozwal.To

1. Treść zadania.

Naszym zadaniem było rozwiązanie zagadek programistycznych umieszczonych na stronie Rozwal.To. Naszym celem było uzyskanie 100 punktów. Poniżej zaprezentowane zostaną rozwiązania poszczególnych etapów.

2. Rozwal.To.

- Zerówka 1

Opis zadania: Jak tego nie rozwalisz - usuń konto.

Rozwiązanie: Wystarczy podejrzeć źródło strony i odkryć hasło ukryte znakami nowych linii.

Hasło: ROZWAL_{DontMessWithZohan}.

Punkty: 1 pkt

- Zerówka 5

Opis zadania: Typowa flaga za 1 p.

Rozwiązanie: W źródle należy odnaleźć funkcję sprawdzającą hasło. Należy uważać na wielkość liter.

Hasło: ROZWAL_{ILikeBiscuits}

Punkty: 1 pkt

- Crypto 3

Opis zadania: Bob uwielbia xorować.

Rozwiązanie: Wiemy, że text zaszyfrowany jest metodą XOR z użyciem jednobajtowego klucza. Możliwości jest tylko 255, więc prosty program metodą brute force rozwiąże zagadkę bezproblemowo. Poniżej zaprezentowana jest listing kodu funkcji deszyfrującej.

```
        static void Main(string[] args)
        {
            string text =
"GCg7Ozs7Oy01e3oNMz4gP3ogP3ovPjs2NXoZM3opMz96KDUgKSAjPCg1LTs5"
                + "ei4/MSkueiA7KSAjPCg1LTs0I3oqNTA/PiM0OSAjN3o4OzAuPzd0ehQ1ej41"
                + "OCg7dno8Njs9O3ouNWB6CBUADRsWBSEJMzQ9Nj8CNSgYIy4/GTMqMj8oJw==";

            var base64EncodedBytes = System.Convert.FromBase64String(text);

            var xortext = System.Text.Encoding.UTF8.GetString(base64EncodedBytes);

            char[] array = xortext.ToCharArray();

            char[] newarray = new char[array.Length];
```

```
            string newstring = string.Empty;

            byte b;

            for (int i = 0; i < 255; i++)
            {
                b = (byte)i;

                for (int j = 0; j < array.Length; j++)
                {
                    newarray[j] = (char)((byte)array[j] ^ b);
                }

                newstring = new string(newarray);
                if (newstring.Contains("ROZWAL_"))
                {
                    Console.WriteLine(b);
                    Console.WriteLine(newstring);
                    Console.ReadLine();
                }
            }
        }
```

Listing 1. Deszyfracja XOR.

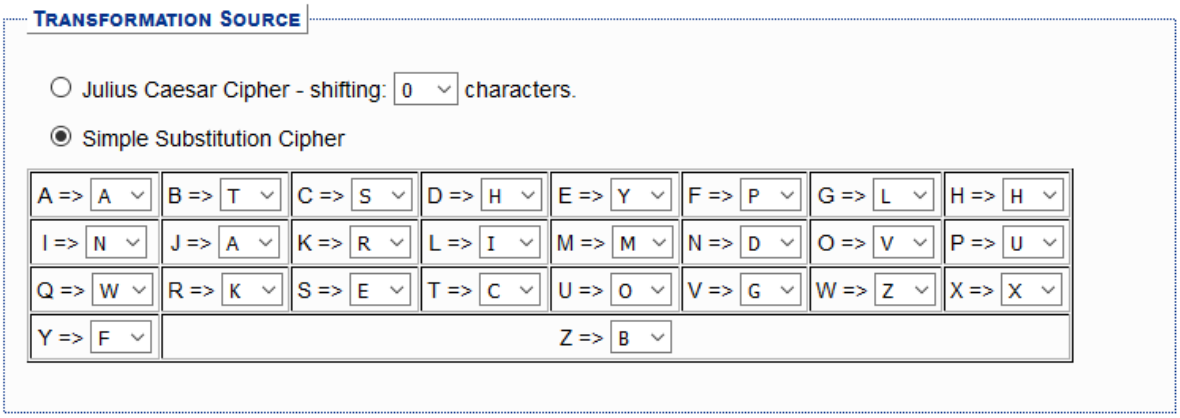
Hasło: ROZWAL_{SingleXorByteCipher}

Punkty: 20 pkt.

- Crypto 6

Opis zadania: Cweyk funcbjqlsiluqe

Rozwiązanie: Wiemy, że tekst jest w języku angielskim. Po wstępnych oględzinach można uznać, że użyty został szyfr podstawieniowy. Analizując poszczególne wyrazy możemy krok po kroku odgadnąć podstawienia. Przy rozwiązazywaniu zadania pomocne okazało się narzędzie dostępne na stronie http://substitution.webmasters.sk/simple-substitution-cipher.php. Poniżej screen z podstawień użytych przeze mnie (rozwiązanie nie jest w pełni poprawne, ale pozwoliło mi na odkrycie hasła).



Rys 1. Reguły dla szyfru podstawieniowego.

Punkty: 20 pkt.

3. Podsumowanie.

Zadania ze strony Rozwal.To okazały się być trudniejsze od tych, które rozwiązywaliśmy poprzednio. Mimo wielu prób nie udało mi się wykonać większej ilości zadań i uzyskać 100 punktów. Mój wynik to 42 punkty.