Universidade Federal do
Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
☎ +55 (87) 3764-5500
http://www.ufape.edu.br

Bacharelado em Ciência da Computação
CCMP3079 Segurança de Redes de Computadores
Prof. Sérgio Mendonça

Atividade Cap. 07
Para 11/12/2023

Nome Completo: _____

Questões retiradas do livro-texto da disciplina.
Conforme conversamos em sala de aula, as atividades devem ser realizadas para apresentação e discussão em sala, sempre nas aulas das quintas-feiras, atribuindo ao estudante uma nota de 0 ou 1 por cada atividade realizada e apresentada.

1. Qual é a diferença entre aleatoriedades estatísticas e imprevisibilidade?
2. Liste considerações de projeto importantes para uma cifra de fluxo.
3. Por que não é desejável reutilizar uma chave de cifra de fluxo?
4. Que operações primitivas são usadas no RC4?
5. Se apanharmos um algoritmo de congruência linear com um componente aditivo de 0:

   $$X_{n+1} = (aX_n) \mod m$$

   então, podemos mostrar que, se m é primo, e se determinado valor de a produz o período máximo de $m-1$, então a^k também produzirá o período máximo, desde que k seja menor que m e que $m-1$ não seja divisível por k. Demonstre isso usando $X_0 = 1$ e $m = 31$, e produzindo as sequências para $ak = 3$, 3^2, 3^3 e 3^4.
6. (a) Qual é o período máximo que pode ser obtido do seguinte gerador?

   $$X_{n+1} = (aX_n) \mod 2^4$$

   (b) Qual deverá ser o valor de a?

   (c) Que restrições são exigidas na semente?
7. Que valor de chave RC4 deixará S inalterado durante a inicialização? Ou seja, após a permutação inicial de S, as entradas de S serão quais aos valores de 0 a 255 na ordem crescente.
8. O algoritmo Blum Blum Shub é baseado na teoria dos resíduos quadráticos e utiliza três números inteiros para realizar os cálculos: p, q e s.

(a) Escolha dois números primos grandes p e q, onde p e q sejam congruentes a 3 mod 4 e não tenham fatores primos comuns. Por exemplo, você pode escolher $p = 499$ e $q = 503$.

(b) Calcule $n = p * q$. Neste caso, n seria igual a $499 * 503 = 250997$.

(c) Escolha um número inteiro s entre 1 e $n - 1$ que seja co-primo com n. Por exemplo, você pode escolher $s = 17$.

(d) Calcule o valor inicial $x_0 = (s^2) \mod n$. Neste caso, x_0 seria igual a $(17^2) \mod 250997 = 289$.

(e) Agora, vamos gerar uma sequência de números aleatórios usando o algoritmo Blum Blum Shub. Para gerar cada número da sequência, use a seguinte fórmula: $x_i = (x_{i-1}^2) \mod n$.

(f) Execute a fórmula várias vezes para gerar uma sequência de números aleatórios. Por exemplo, você pode executar a fórmula 10 vezes para obter 10 números aleatórios.

Aqui está a sequência de números aleatórios gerados usando o algoritmo Blum Blum Shub com os valores do exemplo:

$$289, 253306, 14107, 23546, 67740, 144593, 79829, 46219, 132936, 9863$$

Qual foi a sua sequência?

Livro-texto da disciplina:
STALLINGS, William. Criptografia e segurança de redes. Princípios e práticas, Ed. 6. 2014.