Contents

1. The RC4 stream cipher

Algorithm KSA

```
*Initialization:*
for $i = 0, \cdots, N-1$ do
    $S[i] = i$
end for
$j = 0$
*Scrambling:*
for $i = 0, \cdots, N-1$ do
    $j = j + S[i] + K[i \bmod l]$
end for
return $S$
```

Algorithm PRGA

```
*Initialization*
$i = 0$
$j = 0$
*Keystream generation loop*
i = i + 1
j = j + S[i]
Swap(S[i],S[j])
t = S[i] + S[j]
return $S[t]$
```

1.1 Title of the first subchapter of the first chapter

1.2 Title of the second subchapter of the first chapter

2. Theoretical analysis of the KSA

Notation. $K[a...b] \coloneqq \sum\limits_{i=a}^{b} K[i]$

Lemma 1. *TODO prerekvizita vety 1*

Lemma 2. *TODO prerekvizita vety 1*

Theorem 3. *[1] Assume that during the KSA the index j takes its values uniformly at random from $\mathbb{Z}_N$. Then $\forall 0 \leq i \leq r-1, 1 \leq r \leq N$*

$$\Pr(S_r[i] = K[0...i] + \frac{i(i+1)}{2}) \geq (\frac{N-i}{N})(\frac{N-1}{1})^{\frac{i(i+1)}{2}+r} + \frac{1}{N}$$

Proof. TODO □

Corollary. TODO zobecneni na posledni kolo nebo predchozi vetu rovnou smerovat tam?

TODO tabulka s aktualnimi hodnotami
TODO to same pro InvS
TODO zobecneni na sekvence
TODO inverzni sekvence
TODO vyyiti tohoto na ziskani klice - rovnice

2.1 Substracting equations

Let $i_1 < i_2$. If $C_{i_1} = K[0...i_1]$ and $C_{i_2} = K[0...i_2]$, then we can substract the values and get

$$C_{i_2} - C_{i_1} = K[0...i_2] - K[0...i_1] = K[i_1 + 1...i_2]$$

.

This holds with the product of the individual probabilities of C_i

Conclusion

Bibliography

[1] Paul G. and Maitra S. Rc4 state information at any stage reveals the secret key. *Proceedings of SAC 2007*, 2007.