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

Conclusion