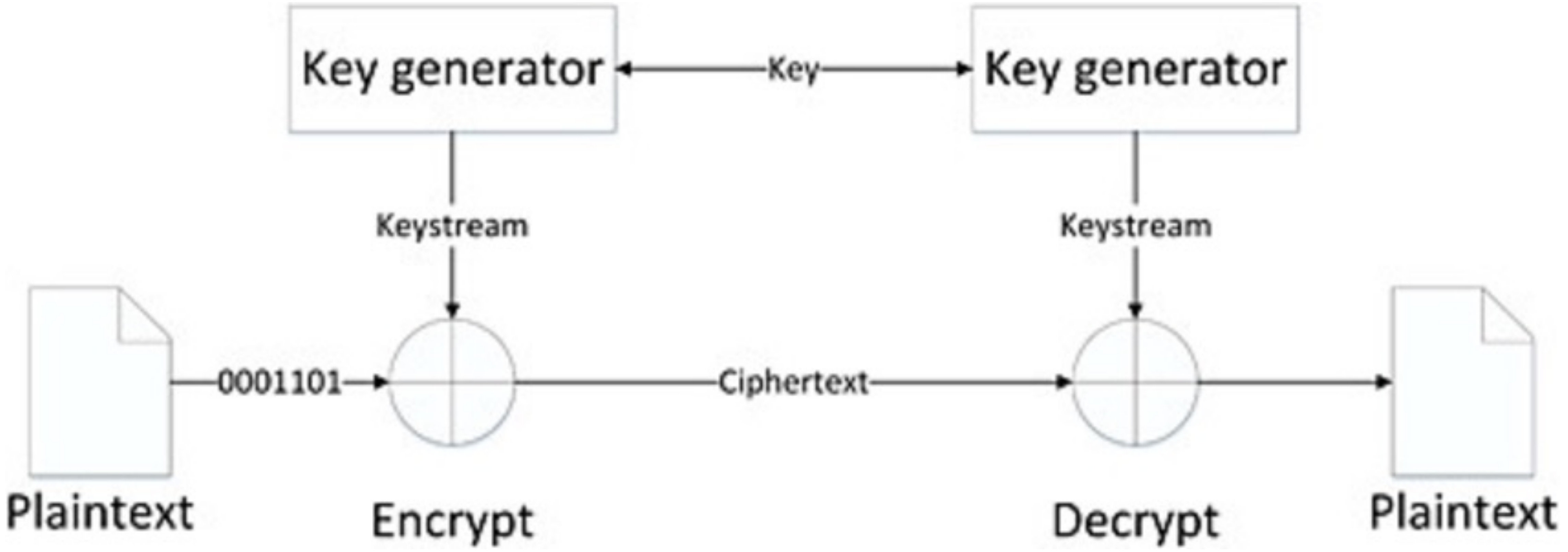
Stream Cipher



- A typical stream cipher encrypts plaintext one byte at a time,
- A Key stream is one that is generated by an algorithm but is unpredictable without knowledge of the input key.
- The output of the generator(**keystream**), is combined one byte at a time with the plaintext stream using the bitwise exclusive-OR (XOR) operation

RC4 Algorithm

RC4 is a stream cipher designed in 1987 by Ron Rivest

1.Uses an array State vector S of length 256(0 to 255)

2.Uses a key array of length 256(0 t0 255)

3.Key encoded with ASCII

Steps in RC4

1.Key Scheduling

2.Key Stream Generator

3.Encryption and Decryption

Key Scheduling

- No.of Iterations=Size of S array
- A temporary vector, T, is also created
- If the length of the key K is 256 bytes, then K is transferred to T

Algorithm

```
/* Initial Permutation of S */
 j = 0;
for i = 0 to 255 do                              S[i]=state vector
 j = (j + S[i] + T[i]) mod 256;                  T[i]=key array
Swap (S[i], S[j]);
```

S array=[0 1 2 3 4 5 6 7]

Key array=[1 2 3 6]

Plain text=[1 2 2 2]

Initialise T array with key

T =[1 2 3 6 1 2 3 6]

Key Stream Generation

Once the S vector is initialized, the input key is no longer used

No.of Iterations=Size of Key

```
/* Stream Generation */
i, j = 0;
 while (true)
 i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
Swap (S[i], S[j]);
t = (S[i] + S[j]) mod 256;
 k = S[t];
```

New Key is generated

Encryption/Decryption

To encrypt, XOR the value k with the next byte of plaintext.

To decrypt, XOR the value k with the next byte of ciphertext

11001100 plaintext !

XOR

01101100 key stream

10100000 ciphertext