RC4 Encryption

Plain_txt: hello world

Key: secret

Cipher_txt: ?

1. Initialize a vector S of 256 bytes from 0 to 255 in ascending order.

S	0	1	2	3	4	...								255

2. Create a temporary vector T with the same size as S. This vector contains a repeated input key.

Key	s	e	c	r	e	t

T	s	e	c	r	e	t	s	e	c	r	e	t	...	

T	115	101	99	114	101	116	115	101	99	114	101	116	...	

3. Use the vector T to produce initial permutation for S starting with S[0] and going through S[255]. S still contains all the numbers from 0 through 255.

T	115	101	99	114	101	116	115	101	99	114	101	116	...	

$T[i]$

$j = j + S[i] + T[i]$

$i = 0$

S	0	1	2	3	4	...								255

$S[i]$ Swap $S[j]$

T	115	101	99	114	101	116	115	101	99	114	101	116	...	

$T[i]$

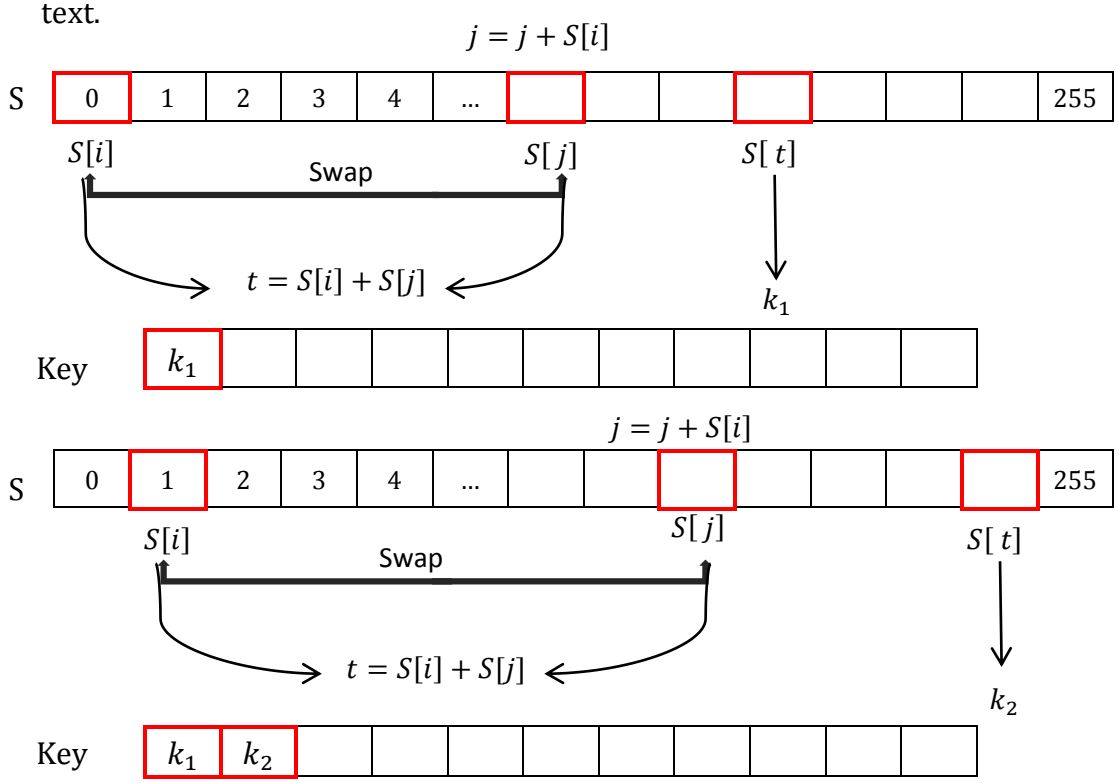
$j = j + S[i] + T[i]$

$i = 1$

S	0	1	2	3	4	...								255

$S[i]$ Swap $S[j]$

4. Stream Generation: Once the vector S is initialized, the vector T is no longer used. In this step, we generate the key that will be used to encrypt the plain text.



5. XOR each byte in the key with the corresponding byte of plain text to generate the cipher text.

Plain_txt	h	e	l	l	o		w	o	r	l	d
Plain_Dec	104	101	108	108	111	32	119	111	114	108	100
Plain_Bin											
⊕ Key_Dec	237	54	210	28	130	164	214	166	50	203	187
Key_Bin											
Cipher_Bin											
Cipher_Dec	133	83	190	112	237	132	161	201	64	167	223
Cipher_txt	…„	S	¾	p	í	„	¡	É	@	§	ß

RC4 Decryption

Cipher_txt: ...S¾pí„¡É@§ß

Key: secret

Plain_txt: hello world

The cipher text is decrypted in the same way as the plain text was encrypted.

1. Initialize a vector S of 256 bytes from 0 to 255 in ascending order.

S	0	1	2	3	4	...								255

2. Create a temporary vector T with the same size as S. This vector contains a repeated input key.

Key	s	e	c	r	e	t

T	s	e	c	r	e	t	s	e	c	r	e	t	...	

T	115	101	99	114	101	116	115	101	99	114	101	116	...	

3. Use the vector T to produce initial permutation for S starting with S[0] and going through S[255]. S still contains all the numbers from 0 through 255.

T	115	101	99	114	101	116	115	101	99	114	101	116	...	

$T[i]$

$$j = j + S[i] + T[i]$$

$i = 0$

S	0	1	2	3	4	...								255

$S[i]$ Swap $S[j]$

T	115	101	99	114	101	116	115	101	99	114	101	116	...	

$T[i]$

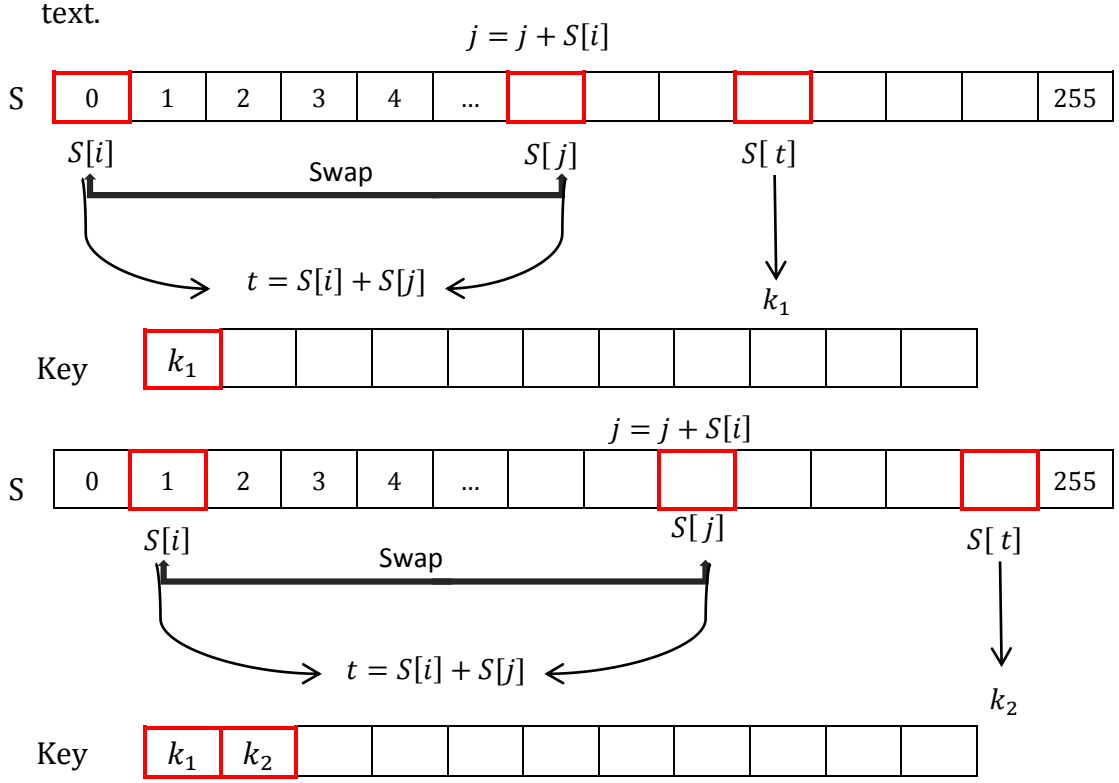
$$j = j + S[i] + T[i]$$

$i = 1$

S	0	1	2	3	4	...								255

$S[i]$ Swap $S[j]$

4. Stream Generation: Once the vector S is initialized, the vector T is no longer used. In this step, we generate the key that will be used to encrypt the plain text.



5. XOR each byte in the key with the corresponding byte of plain text to generate the cipher text.

Cipher_txt	…„	S	¾	p	í	„	¡	É	@	§	ß
Cipher_Dec	133	83	190	112	237	132	161	201	64	167	223
Cipher_Bin											
⊕ Key_Dec	237	54	210	28	130	164	214	166	50	203	187
Key_Bin											
Plain_Bin											
Plain_Dec	104	101	108	108	111	32	119	111	114	108	100
Plain_txt	h	e	l	l	o		w	o	r	l	d