

ClientHs

KEM\_pk

OKEM\_ciphertext

padding

mark

mac

32B b'\x02\_\xa4\xc9\x9[...]

0B b''

77B b'\x9fLk\x88\xed\x[...]

16B b'P\x83\xe4\x0b+\x[...]

16B b'\xc7\xc3{7/\xcf\ [...]

02	5f	a4	c9	9c	64	97	5c	37	63	82	65	00	37	d5	f1
17	d5	2a	4e	84	6a	fd	06	46	29	c6	ee	3b	4c	f5	33

9f	4c	6b	88	ed	b9	4d	ff	d4	b9	30	01	4c	08	9e	78
1e	f7	60	f1	e0	68	7e	86	3e	f5	99	71	9a	bd	6f	a5
60	8e	54	81	4a	c8	d7	75	a2	56	d3	1e	4b	0e	29	3a
02	d3	3c	75	ab	ab	d7	3a	e6	b9	24	c4	c9	5f	5c	2c

af	f2	0f	9f	42	d8	6f	aa	bb	45	c1	fe	17	50	83	e4
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

0b	2b	fd	7b	0c	91	eb	9e	57	04	fd	0b	cd	c7	c3	7b
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

37	2f	cf	d7	b1	45	76	2d	65	98	aa	52	ca
----	----	----	----	----	----	----	----	----	----	----	----	----