1 Byte	Version Number	Public Key
4 Byte	Creation time	
1 Byte	Algorithm (RSA)	
?	Modulus n	
?	Exponent e	
1 Byte	String-to-key-usage (0xFF)	Parameter
(1)	symmetrical algorithm	
(1+1+8+1)	0x03 (iterated and salted string-to-key identifier); identifier of the hash algorithm (for SHA-1, it is 0x02); salt (random data, which are hashed together with the user's passphrase and diversifies thus derived symmetrical key); the number of hashed octets of the data (the so-called "count")	
(8-16)	Initialisation vector IV	
2 + 256	Prefix + exponent d	Private Key
2 + 128	Prefix + prime p	
2 + 128	Prefix + prime q	
2 + 128	Prefix + pInv	
2	checksum, arithmetic sum of previous octets (prefixes and numbers $d, p, q, pInv$) as plaintext, modulo 65536 (in version 4 encrypted, in version 3 not encrypted)	