1 Byte	Version number	Public Key
4 Byte	Creation time	
1 Byte	Algorithm (DSA)	
2+128	Prime number p	
2+20	Prime number q	
2+128	Element g	
2+128	Public key y	
1 Byte	String-to-key-usage (0xFF)	Parameters
(1)	Symmetric encryption algorithm	
(1+1+8+1)	Identifier of the hash algorithm (e.g. 0x02 for SHA-1); salt (random data, which is used together with the user's passphrase in the key derivation function); number of hashed octets of the data (the so-called *count*)	
(8 bis 16)	Initialisation vector IV	
2 20 2	Prefix of x (unencrypted in version 3, encrypted in version 4) Integer x (encrypted in versions 3 and 4) Checksum: arithmetic sum of 22 previous octets as plaintext modulo 65536 (unencrypted in version 3, encrypted in version 4)	Private Key