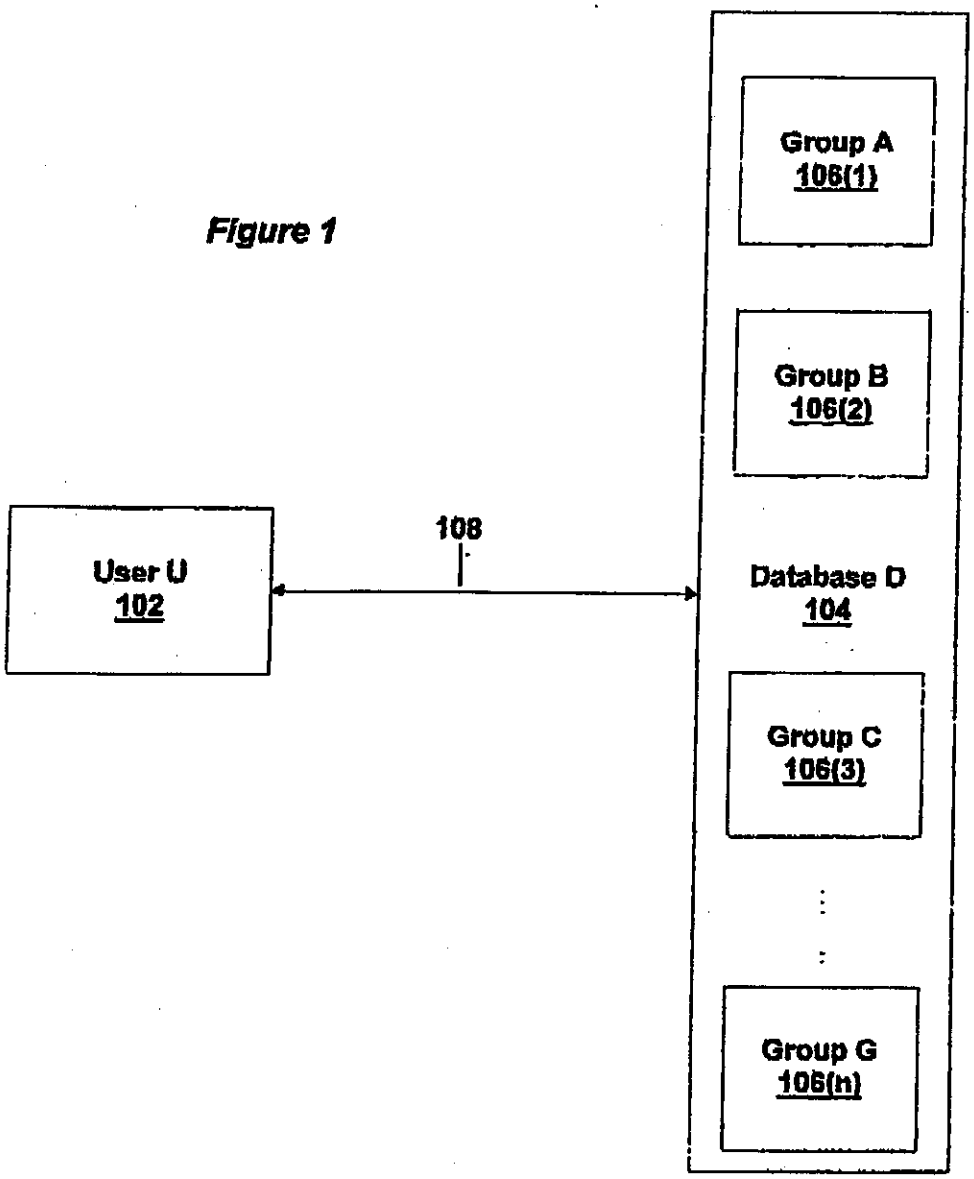
12 OCT 2004



*Figure 1*



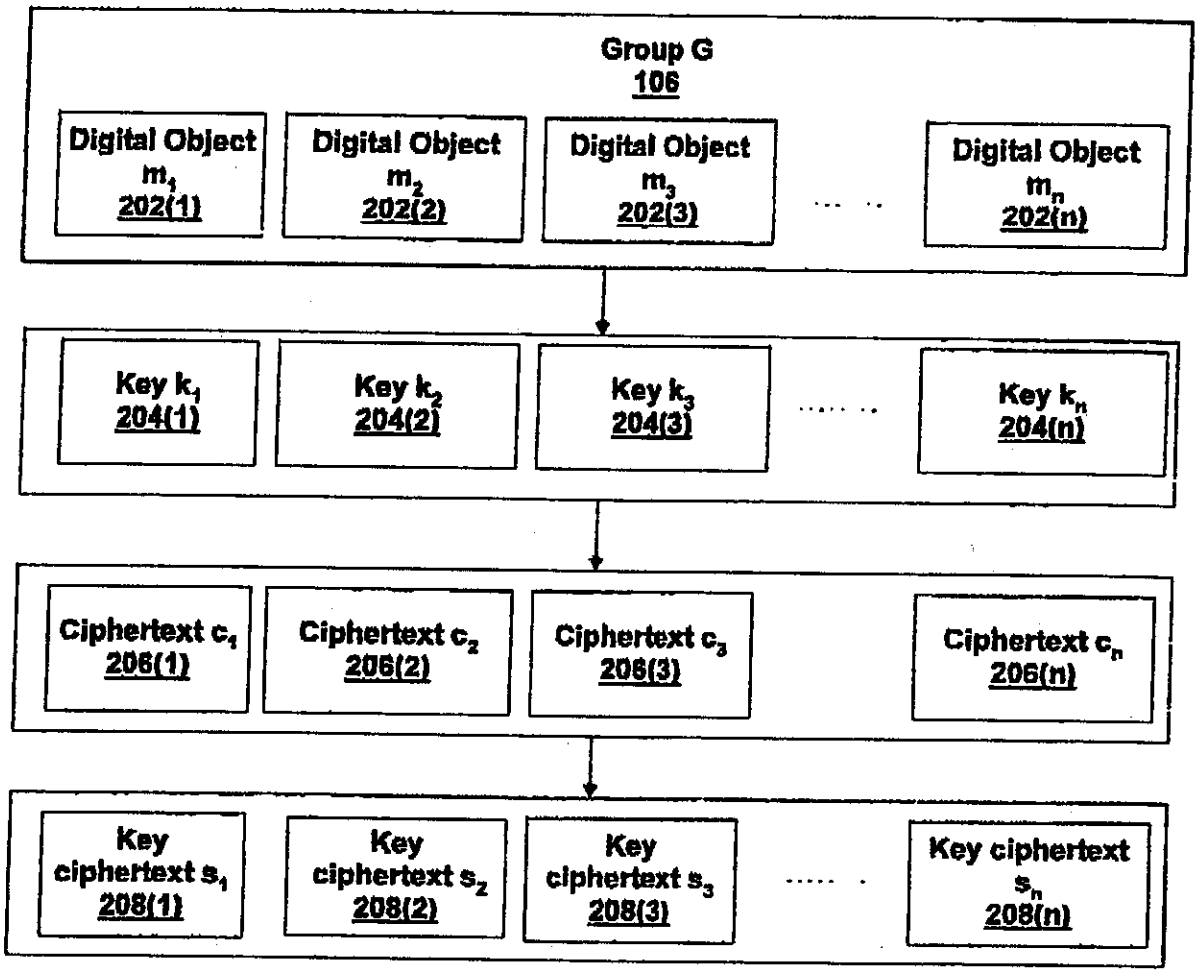

Group G
106
Digital Object $m_1$ 202(1)
Digital Object $m_2$ 202(2)
Digital Object $m_3$ 202(3)
Digital Object $m_n$ 202(n)
Key $k_1$ 204(1)
Key $k_2$ 204(2)
Key $k_3$ 204(3)
Key $k_n$ 204(n)
Ciphertext $c_1$ 206(1)
Ciphertext $c_2$ 206(2)
Ciphertext $c_3$ 206(3)
Ciphertext $c_n$ 206(n)
Key ciphertext $s_1$ 208(1)
Key ciphertext $s_2$ 208(2)
Key ciphertext $s_3$ 208(3)
Key ciphertext $s_n$ 208(n)

*Figure 2*

*Figure 3*

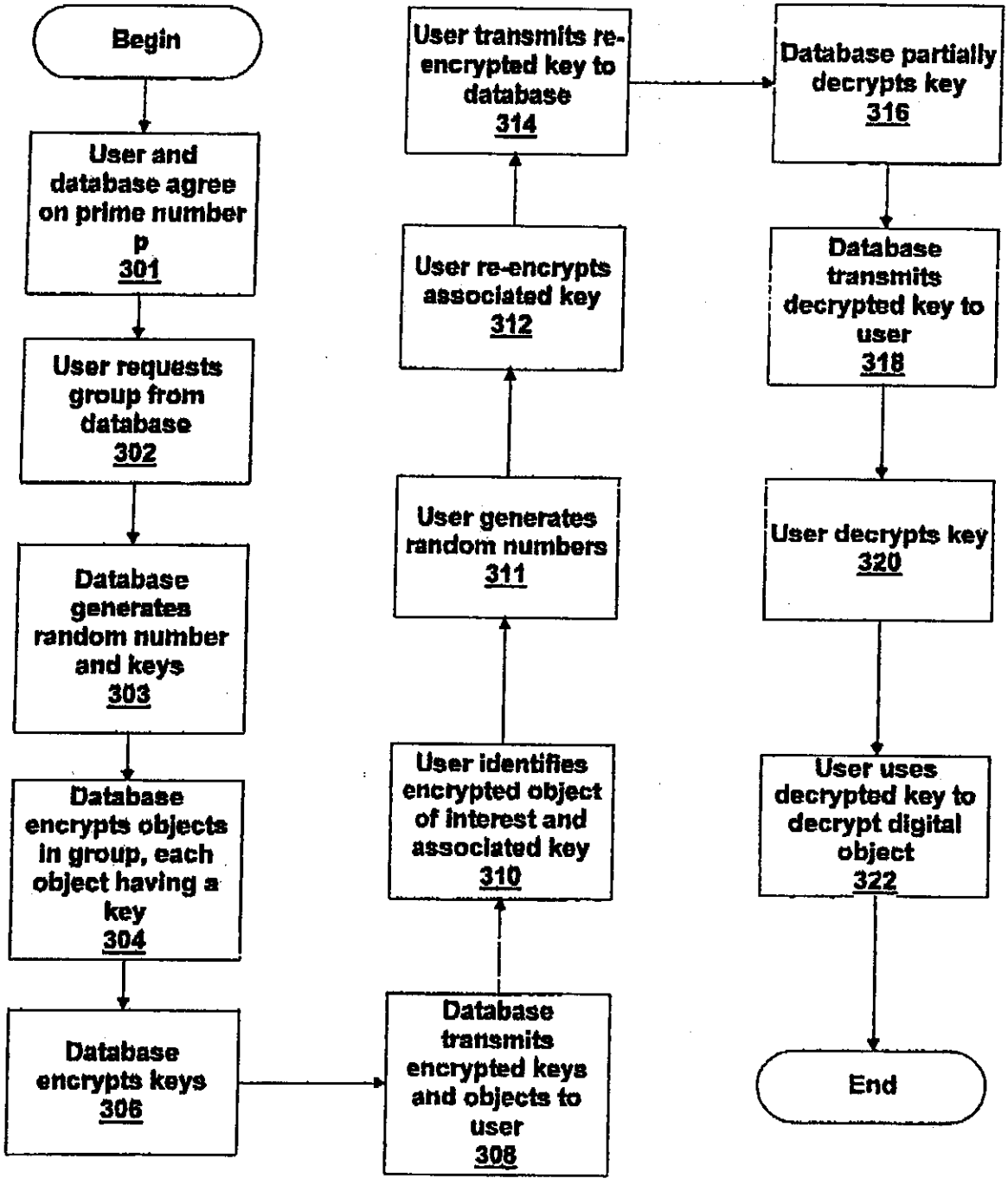
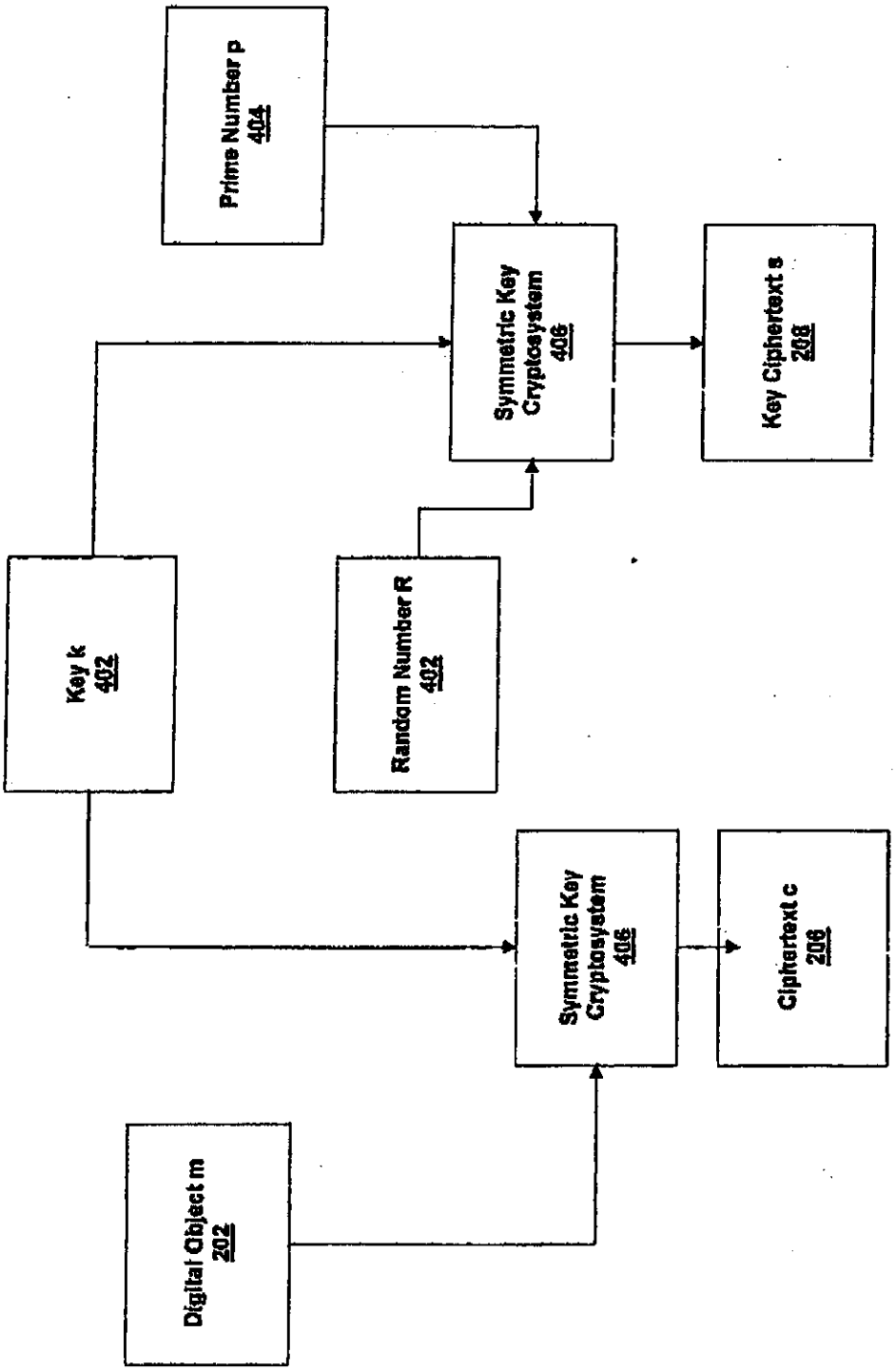

Begin
User and database agree on prime number p
301
User requests group from database
302
Database generates random number and keys
303
Database encrypts objects in group, each object having a key
304
Database encrypts keys
306
Database transmits encrypted keys and objects to user
308
User identifies encrypted object of interest and associated key
310
User generates random numbers
311
User re-encrypts associated key
312
User transmits re-encrypted key to database
314
Database partially decrypts key
316
Database transmits decrypted key to user
318
User decrypts key
320
User uses decrypted key to decrypt digital object
322
End

Figure 4


Prime Number p
404
Symmetric Key Cryptosystem
406
Key Ciphertext s
208
Key k
402
Random Number R
402
Symmetric Key Cryptosystem
406
Ciphertext c
206
Digital Object m
202

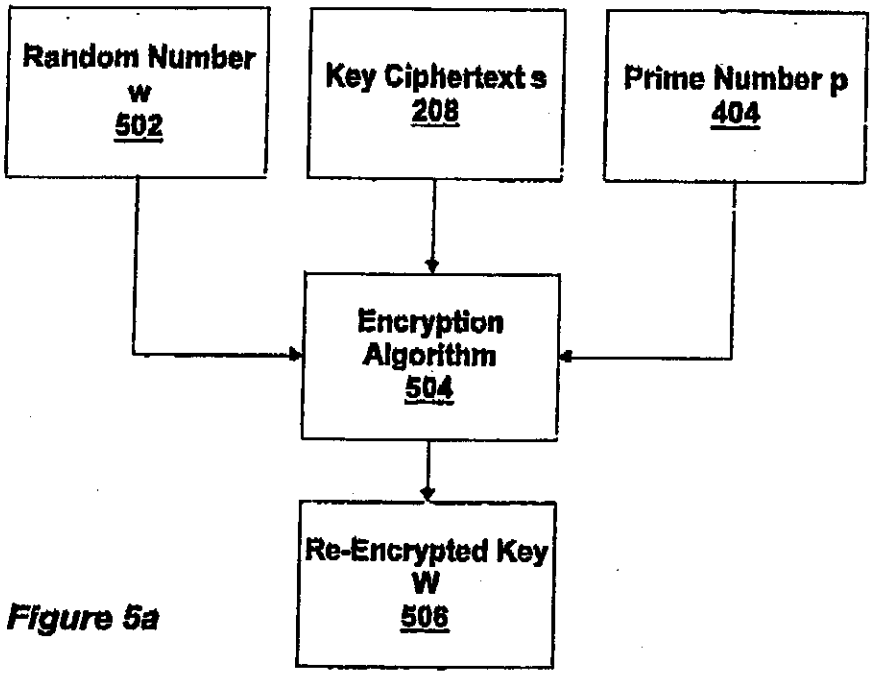



*Figure 5a*

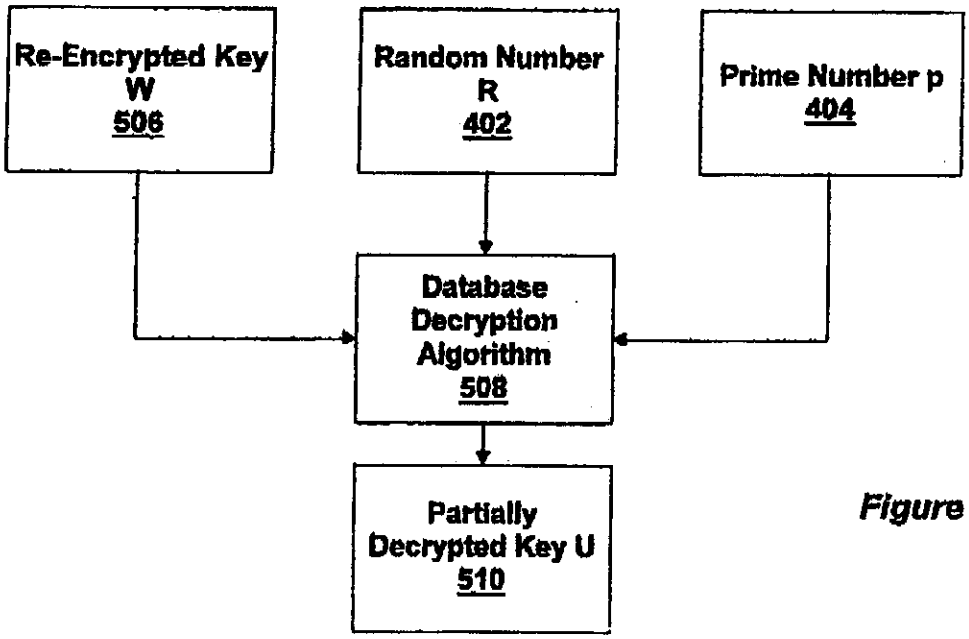



*Figure 5b*

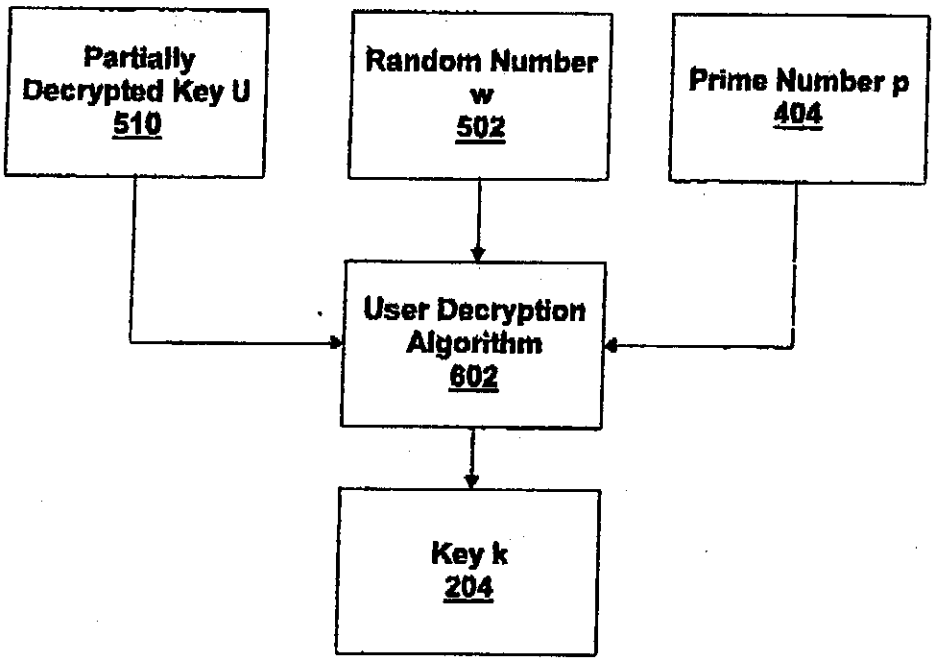



Figure 6a

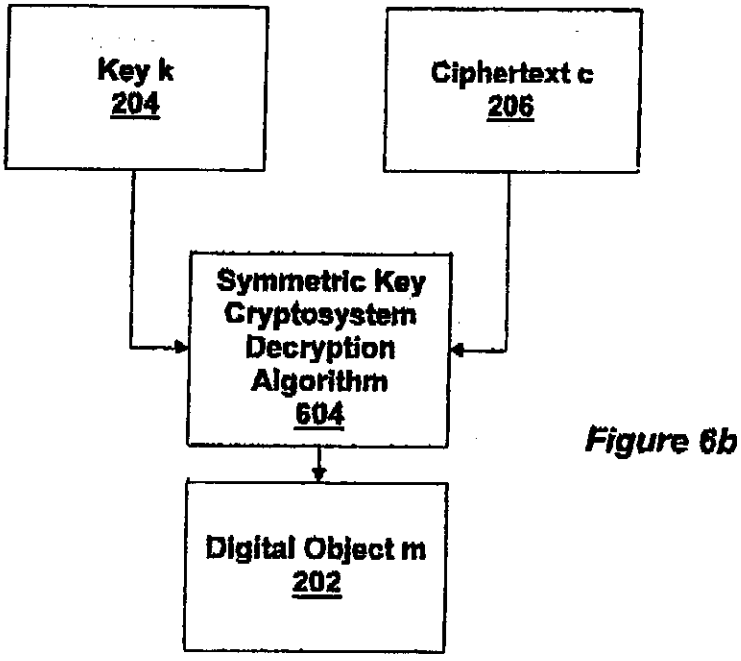



Figure 6b

12 OCT 2004

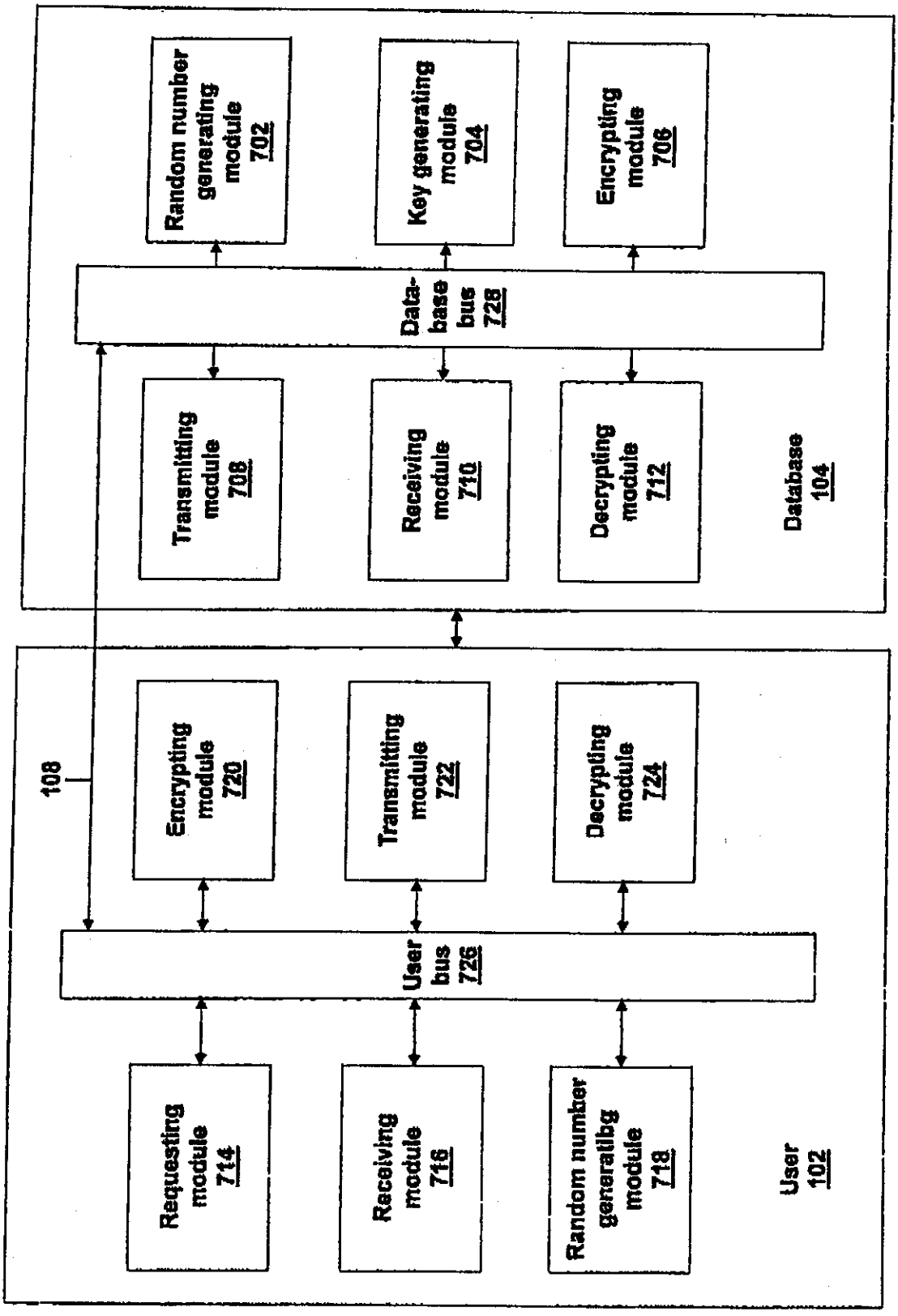



Figure 7