

聊聊什么是 SM2 和 RSA 密钥

某王朝边关发生战争，皇派大将军守土抗敌。军情紧急，战报不容泄露，然则国土平安已久，各方面被敌方渗透厉害，敌方奸细无处不在，前不久查到大将军的好朋友和小妾也都和敌方有私下来往，某信使也叛变投敌。将军与皇之间的情报交换必须稳妥可靠才行。怎么办？

思虑一番，皇命人制造了一批特特殊的盒子和钥匙，其特殊性是：1、所有钥匙只对某个盒子的锁只具备**上锁和开锁的单一功能**，不同时具备上锁和开锁的功能；2、上锁后的盒子**只能通过开锁的钥匙打开**，否则信息报废。

皇拿出一对金钥匙，对大将军说：一、我要是有信息要给你，我就用这把上锁的金钥匙锁盒子，你收到盒子，用这把开锁的金钥匙打开。二、如果你有信息要给我，你用这把上锁的银钥匙锁上盒子，我收到后用这把开锁的银钥匙打开。

于是，皇手上有一把上锁的金钥匙和一把开锁的银钥匙，而大将军手中就有一把开锁的金钥匙和一把上锁的银钥匙。

结合 SM2 密钥来说，就是：

金上锁钥匙：

012C1C5C364694ECB6859602FB90D9EA3091A4D83A4746C5B4E243E89F96C899

金开锁钥匙：

044757F676AA885B97457C0DB47CF8EC324ED138783C92CB5AAB27A978CAE6FEB01B23F
20CBE85797003DBE84AFDF5B2A7D2BE6FC01593EB1CF7883FEA0C91EA3E

银上锁钥匙：

4462BDEDA77B6FC3FA3C0A17F8A615442C57D11D9B2A017A84B5A764F680339C

银开锁钥匙：

0495001736072BDD034D445C9E09D778BE0E0CCBFAD34C24218059745D86990E79C376B
8857F2250CA52A4FF85BC221A1C86C6F0D57DE61215896DAD275279E561

皇和将军交换后，

皇手上的钥匙是：

金上锁钥匙：

012C1C5C364694ECB6859602FB90D9EA3091A4D83A4746C5B4E243E89F96C899

银开锁钥匙：

0495001736072BDD034D445C9E09D778BE0E0CCBFAD34C24218059745D86990E79C376B
8857F2250CA52A4FF85BC221A1C86C6F0D57DE61215896DAD275279E561

大将军手上的钥匙是：

银上锁钥匙：

4462BDEDA77B6FC3FA3C0A17F8A615442C57D11D9B2A017A84B5A764F680339C

金开锁钥匙：

044757F676AA885B97457C0DB47CF8EC324ED138783C92CB5AAB27A978CAE6FEB01B23F
20CBE85797003DBE84AFDF5B2A7D2BE6FC01593EB1CF7883FEA0C91EA3E

这样皇和大将军可以让信息在两人之间保密安全送达。

假如你是大将军，你手上有这样两个密钥，一个是金，一个是银，它们并不配对。这时候，你用银钥匙上锁，你用金钥匙能开锁吗？显然不能。