BouncyCastle的库生成RSA密钥对时，私钥d因子跟p/q对应不上（或者说，由p/q/e计算出来的d’不等于d）。然而，**对明文用（n, e）加密的结果，用（n, d）和（n, d’）都能正确解密。**

举例如下：

下面这组数据是后台服务，用BC算法库生成的RSA密钥对的所有因子。其中rsa\_d和p/q/e不能匹配。

        "rsa\_dp": "b3994ba64f46a3930c707bc3f99851072e96c56cb106407714c84bb7ec54488a8ec8eaeb030be6e9e3e312dcf75cf9a4711fda0717ac44de0974d2653837685d",

        "rsa\_dq": "3a2605cd0704856c517118d2beddc0cbcf5a1ca3768f3637d5ab8010fa40da5ed0e57c56fe3ceeda712a0ab757eea3c7840507779547e530e335a2f40bb99d69",

        "rsa\_p": "f8cad911fdd737311433dc7be0f1171fd9076443de6162f4759cd97109dc346aa90a5db85e0f9dc3f3a56ec99646fa485f58720f873df5d163efead7be9d8da3",

        "rsa\_q": "f4a1d5ea309a48c7f17f007d8bdb50a5ea1396a79b9a529c936e08af48c3b3160aa760ddd3f50a57c13b7445da4d2aa9eb1b0a7e9d8e1fc3231c44a7561b0905",

        "rsa\_n": "edbe9e5c0984210fe69ca9163e2640b4e240b5f7b623bd3105b593d41cd073a7392c874d144402b978e94bf8333c05b32849915b7478557d07b9118f6261014f144bb0f1a3b5aacefac37ea8aad2eb43b4639eed2f1d506f43b560f30367ad70a607e7ce4ef7e40a6099a5662eb2286cb51e018ffea1d1ed9af5e571f53f7f2f",

        "rsa\_qinv": "3c5842e34f10a133c011d36dba0b8bd2068cae45690cf86d1e811d975b0b5b266379c55fcfee4df4d555d477a37ea59d31d6cd24f86626ed7952b3da1ce0f703",

        "rsa\_d": "42f3a37517d8f5d69c8311bb09d58bf364a4049ab5d86ab71b7c7f1d04e04f31909051aa0b42fbe16f8383b969f44546a6d9d0ed88673aebf2f8d35125cb5baa767fe6f55108d96757944f74226b832c3c7ed0710aa9640ba149d25d531b6f4a9b5c584f4d17d290ec1b23df79baca0ff769fdfaff75898d2c666caef13c0cd",

        "rsa\_e": "10001",

由上面的p/q/e数据计算出的 n/d’/dp/dq/qinv，除了d’之外，其它四项数据均与上面对应因子相等。计算的d’为：

        "rsa\_d’": {

            "hex": "7b0e8965563f9fe55d1685a6cfb07919a76a9b45866f6543f49291dbdeb63ec6b59f48c12ad6311ad36cde37b03d472dfe9265bc92c29e6d430c15fcc38d36613ad77f6a0fb2a301700195cee129f9f1bc6c3f07eb3b63afd769dc8f2d9599eca2e0da21034b1b20649e136956aaae5e34cbe2609ce236c55cbb41c45f573511"

        },