链滴

Java 代码实现 TOTP 算法

作者：jerryhwq

原文链接：https://ld246.com/article/1515494608199

来源网站：链滴

TOTP算法是目前手机令牌客户端动态密码采用的算法,算法实现起来比较简单:

```
/**
 * @param key 密钥,如用户名等
 * @param length 需要的长度
 * @param step 步长(有效期)
 * @param timestamp 时间戳
 * @return 动态密码
 * @throws NoSuchAlgorithmException
 * @throws InvalidKeyException
 */
public static String generateTOTP(String key, int length, long step, long timestamp) throws N
SuchAlgorithmException, InvalidKeyException {
    SecretKeySpec signingKey = new SecretKeySpec(key.getBytes(), "RAW");
    Mac mac = Mac.getInstance("HmacSHA1");
    mac.init(signingKey);
    // 将当前时间除步长作为消息文本进行hmac-sha1加密
    String message = String.valueOf(timestamp / step);
    byte[] hash = mac.doFinal(message.getBytes());
    // 取最低四位组成的数字作为偏移量offset
    int offset = hash[hash.length - 1] & 0xf;
    // 取从最高为开始偏移offset的4字节同时去掉最高位组成的数字
    int num = ((hash[offset] & 0x7f) << 24) | ((hash[offset + 1] & 0xff) << 16) | ((hash[offset + 2
 & 0xff) << 8) | (hash[offset + 3] & 0xff);
    // 将得到的数字十进制形式最后几位作为最终的结果，如果位数不足高位用0补齐
    String finalKey = String.format(String.format("%%0%dd", length), num);
    if (finalKey.length() > length) {
        finalKey = finalKey.substring(finalKey.length() - length);
    }
    return finalKey;
}
```