**第四次作业：密码算法实现**

计21 2012011401 张梦豪

*一、编程实现SHA-1、SHA-2、SHA-3、SM3算法， 对每个算法给出以下字符串的杂凑值，并提交每个算法的C语言程序 （列出每步的中间结果，如SM3有64步，1-3需将需将每步的输出值列出。）*

*1、 空字符串，也就是长度为0的字符串。*

解：所有程序见目录1底下。

SHA-1：

da39a3ee5e6b4b0d3255bfef95601890afd80709

SHA-2-256：

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

SHA-2-512：

cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e

SHA-3-256：

a7ffc6f8bf1ed76651c14756a061d662f580ff4de43b49fa82d80a4b80f8434a

SHA-3-512：

a69f73cca23a9ac5c8b567dc185a756e97c982164fe25859e0d1dcc1475c80a615b2123af1f5f94c11e3e9402c3ac558f500199d95b6d3e301758586281dcd26SM3

SM3：

1ab21d8355cfa17f8e61194831e81a8f22bec8c728fefb747ed035eb5082aa2b

*2、 3个字节的字符串’abc’, 等价于ASCII字符串’01100001 01100010 011000011’*

解：SHA-1：

a9993e364706816aba3e25717850c26c9cd0d89d

SHA-2-256：

ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad

SHA-2-512：

ddaf35a193617abacc417349ae20413112e6fa4e89a97ea20a9eeee64b55d39a2192992a274fc1a836ba3c23a3feebbd454d4423643ce80e2a9ac94fa54ca49f

SHA-3-256：

3a985da74fe225b2045c172d6bd390bd855f086e3e9d525b46bfe24511431532

SHA-3-512：

b751850b1a57168a5693cd924b6b096e08f621827444f70d884f5d0240d2712e10e116e9192af3c91a7ec57647e3934057340b4cf408d5a56592f8274eec53f0

SM3：

66c7f0f462eeedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0

*3、 每位同学姓名的全拼加学号。如 姓名：于红波 学号: 2007990061, 则输入消息为’yuhongbo2007990061’。*

解：加密的消息为：zhangmenghao2012011401

SHA-1：

d7207e22ecd5b6effb4b0867f470b6700bf8398a

SHA-2-256：

94e6fae2b57ca334f1593419e417981c44f689efc2a5e8dcaf56300b80d36d2c

SHA-2-512：

9123e321a5c05e0a1fcbfe6f07a2739282f4d3280725670ed63e41687ffe1b9168341370b28d1e2f8432cf735459a15a73f80fd3b0ceec6a343b9bd11d3068f5

SHA-3-256：

68091e7b282f7b37d18d8a98a1ee221d1900f777d85a460092e97aca82746536

SHA-3-512：

9f8d95e6e8d83b4336e84f39a71729b0c4a221549e40abaa1a0e17d6bee81fc3adace9e3be6a4300f30c47bb32dbef1d562068fb6c464595f7a60670459d4924

SM3：

1f15cffc4d003898648ae779ee9d15f48d123932b772915168c28716e5a8705

*4、 62个byte的字符串*

*ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789*

解：SHA-1：

761c457bf73b14d27e9e9265c46f4b4dda11f940

SHA-2-256：

db4bfcbd4da0cd85a60c3c37d3fbd8805c77f15fc6b1fdfe614ee0a7c8fdb4c0

SHA-2-512：

1e07be23c26a86ea37ea810c8ec7809352515a970e9253c26f536cfc7a9996c45c8370583e0a78fa4a90041d71a4ceab7423f19c71b9d5a3e01249f0bebd5894

SHA-3-256：

a79d6a9da47f04a3b9a9323ec9991f2105d4c78a7bc7beeb103855a7a11dfb9f

SHA-3-512：

d1db17b4745b255e5eb159f66593cc9c143850979fc7a3951796aba80165aab536b46174ce19e3f707f0e5c6487f5f03084bc0ec9461691ef20113e42ad28163SM3

SM3：

2971d10c8842b70c979e55063480c50bacffd90e98e2e60d2512ab8abfdfcec5

*5、 将字符’a’重复106次*

解：SHA-1：

34aa973cd4c4daa4f61eeb2bdbad27316534016f

SHA-2-256：

cdc76e5c9914fb9281a1c7e284d73e67f1809a48a497200e46d39ccc7112cd0

SHA-2-512：

e718483d0ce769644e2e42c7bc15b4638e1f98b13b2044285632a803afa973ebde0ff244877ea60a4cb0432ce577c31beb009c5c2c49aa2e4eadb217ad8cc09b

SHA-3-256：

5c8875ae474a3634ba4fd55ec85bffd661f32aca75c6d699d0cdcb6c115891c1

SHA-3-512：

3c3a876da14034ab60627c077bb98f7e120a2a5370212dffb3385a18d4f38859ed311d0a9d5141ce9cc5c66ee689b266a8aa18ace8282a0e0db596c90b0a7b87SM3

SM3：

c8aaf89429554029e231941a2acc0ad61ff2a5acd8fadd25847a3a732b3b02c3

*二、使用DES、AES、SM4分别在CBC、OFB、CTR模式下加密‘aaaaaaa…..’ (将字符a重复106次), 算法中使用的IV可设置为0。（提交程序和密文）*

解：我在这里使用的密钥为12345678或者它的循环，程序和密文见目录2底下相关目录。

*三、使用AES-GCM对字符串*

*ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789*

*进行认证加密。附加数据A设为空字符串。（提交程序、密文和认证码）*

解： 在这里，我将IV设置为0，密钥设置也设置为0。

密文：

CF355E5DB0BCDAECFDC1FDA95DD7B6CC96881A460D10026FF5FB256CAA1702C56515161B67853391769B396DB421E63ADC13A24B12EBAD30DC7AB902ABAB

认证码：

7f23c45670c94597c87d92e8f66f59c3