

Cryptography Final

You may use the textbook and course notes and only the Wikipedia pages for Reed-Solomon codes, Hamming codes and the El Gamal crypto system.

You can use no other material and may only discuss the problems with the instructor and no one else.

1. Suppose we have codes \mathcal{C}_1 and \mathcal{C}_2 . Code \mathcal{C}_1 has length n_1 , m_1 messages, distance d_1 and alphabet size q_1 . Code \mathcal{C}_2 has similar parameters n_2 , m_2 , d_2 and q_2 . Assume $m_2 \geq q_1$ and $q_2 < q_1$.

The concatenated code \mathcal{C} is made by taking a codeword from \mathcal{C}_1 and replacing every alphabet symbol with a different codeword from \mathcal{C}_2 .

For example suppose we have

$$\mathcal{C}_1 = \{abc, bca, cab\}$$

and

$$\mathcal{C}_2 = \{001, 100, 010\}$$

then we would have

$$\mathcal{C} = \{001100010, 100010001, 010001100\}$$

by replacing the a in each codeword of \mathcal{C}_1 with 001, b with 100 and c with 010.

- (a) In general, what is the length n , number of messages m , distance d , alphabet size q and rate of code \mathcal{C} as functions of $n_1, m_1, d_1, q_1, n_2, m_2, d_2$ and q_2 .
- (b) Consider the concatenation of the Reed-Solomon code with Field size 11 and degree 8 and the [15, 11] binary Hamming code.
Is this concatenated code a linear code? A binary code?
Calculate the distance d and rate of this code.
- (c) What are the advantages of using a concatenated code?

TEST CONTINUES ON NEXT PAGE

2. Below we give a protocol is used to determine if one El Gamal encryption of a cybertext is a reencryption of another. This protocol can be used to implement a cryptographic voting scheme.

Fix a prime p , α a primitive root of p and $\beta = \alpha^a$. The public key is (p, α, β) and the private key is a .

Except as noted, all of the math in this problem is done mod p .

Let $c_1 = (\gamma_1, \eta_1) = (\alpha^t, m_1\beta^t)$ and $c_2 = (\gamma_2, \eta_2) = (\alpha^u, m_2\beta^u)$. We say c_2 is a reencryption of c_1 if $m_1 = m_2$.

Let

$$(a_1, a_2, b_1, b_2) = \left(\alpha, \beta, \frac{\gamma_2}{\gamma_1}, \frac{\eta_2}{\eta_1}\right) = \left(\alpha, \beta, \alpha^{u-t}, \frac{m_2}{m_1}\beta^{u-t}\right).$$

Suppose Peggy knows $r = u - t$. Consider the following protocol.

Peggy: Pick random s . Let $v = a_1^s$ and $w = a_2^s$. Send v and w to Victor.

Victor: Pick random c and send c to Peggy.

Peggy: Let $z = s + cr \pmod{p-1}$ and send z to Victor.

Victor checks that both $a_1^z = vb_1^c$ and $a_2^z = wb_2^c$.

- (a) Show that c_2 is a reencryption of c_1 if and only if $\log_{a_1}(b_1) = \log_{a_2}(b_2)$.
- (b) Show that if c_2 is a reencryption of c_1 and Peggy follows protocol then Victor's tests will always pass.
- (c) Show that if c_2 is not a reencryption of c_1 then no matter what Peggy does, Victor's tests will not both pass with high probability.
- (d) Show that if c_2 is a reencryption of c_1 and Victor follows protocol then Victor learns nothing about r .
- (e) Show that if Victor sends c before Peggy sends v and w then even if c_2 is not a reencryption of c_1 then Peggy can cheat and always ensure Victor's test will pass.