

# RSA, POLYNOMIALS, SECRET SHARING, ERASURE ERRORS 4

---

COMPUTER SCIENCE MENTORS 70

Feb 20 to Feb 27, 2017

---

## 1 RSA

---

### 1.1 Questions

---

#### 1. How does RSA work?

- a. Alice wants to send Bob a message  $m = 5$  using his public key ( $n = 26, e = 11$ ). What cipher text  $E(m)$  will Alice send?
  
  
  
  
  
  
  
  
  
  
- b. What is the value of  $d$  (Bobs private key) in this scheme? Note that traditional RSA schemes use much larger prime numbers, so its harder to break  $n$  down into its prime factors than it is in this problem.

2. In RSA, if Alice wants to send a confidential message to Bob, she uses Bob's public key to encode it. Then Bob uses his private key to decode the message. Suppose that Bob chose  $N = 77$ . And then Bob chose  $e = 3$  so his public key is  $(3, 77)$ . And then Bob chose  $d = 26$  so his private key is  $(26, 77)$ .

Will this work for encoding and decoding messages? If not, where did Bob first go wrong in the above sequence of steps and what is the consequence of that error? If it does work, then show that it works.

### 3. Coin tosses over text messages

You and one of your friends want to get your hands on the new gadget that's coming out. One of you has to wait in line overnight so that you have a chance to get the gadgets while they last. In order to decide who this person should be, you both agree to toss a coin. But you won't meet each other until the day of the actual sale and you have to settle this coin toss over text messages (using your old gadgets). Obviously neither of you trusts the other person to simply do the coin toss and report the results.

How can you use RSA to help fix the problem?

## 2 Polynomials

---

### 2.1 Introduction

---

1. There is a unique polynomial of degree  $n - 1$  such that  $P(i) = m_i$  for each packet  $m_1, \dots, m_n$
2. To account for errors we send  $c_1 = P(1), \dots, c_{n+j} = P(n + j)$
3. If polynomial  $P(x)$  has degree  $n - 1$  then we can uniquely reconstruct it from any  $n$  distinct points.
4. If a polynomial  $P(x)$  has degree  $n - 1$  then it can be uniquely described by its  $n$  coefficients

### 2.2 Questions

---

1. Define the sequence of polynomials by  $P_0(x) = x + 12$ ,  $P_1(x) = x^2 - 5x + 5$  and  $P_n(x) = xP_{n-2}(x) - P_{n-1}(x)$ . (For instance,  $P_2(x) = 17x - 5$  and  $P_3(x) = x^3 - 5x^2 - 12x + 5$ .)
  - (a) Show that  $P_n(7) \equiv 0 \pmod{19}$  for every  $n \in \mathbb{N}$ .
  - (b) Show that, for every prime  $q$ , if  $P_{2013}(x) \not\equiv 0 \pmod{q}$ , then  $P_{2013}(x)$  has at most 2013 roots modulo  $q$ .

## 3 Secret Sharing

---

### 3.1 Questions

---

1. Suppose the Oral Exam questions are created by 2 TAs and 3 Readers. The answers are all encrypted and we know that:
  - (a) Both TAs should be able to access the answers
  - (b) All 3 Readers can also access the answers
  - (c) One TA and one Reader should also be able to do the same

Design a secret sharing scheme to make this work.

2. The United Nations (for the purposes of this question) consists of  $n$  countries, each having  $k$  representatives. A vault in the United Nations can be opened with a secret combination  $s$ . The vault should only be opened in one of two situations. First, it can be opened if all  $n$  countries in the UN help. Second, it can be opened if at least  $m$  countries get together with the Secretary General of the UN.

Propose a scheme that gives private information to the Secretary General and  $n$  countries so that  $s$  can only be recovered under either one of the two specified conditions.

## 4 Erasure Errors

### 4.1 Introduction

We want to send  $n$  packets and we know that  $k$  packets could get lost.

3
---

1
---

5
---

0
---

 $\rightarrow$ 

--

1
---

5
---

--

How many more points does Alice need to send to account for  $k$  possible errors? \_\_

What degree will the resulting polynomial be? \_\_

How large should  $q$  be if Alice is sending  $n$  packets with  $k$  erasure errors, where each packet has  $b$  bits?

What would happen if Alice instead send  $n + k - 1$ ? Why will Bob be unable to recover the message?

### 4.2 Questions

1. Suppose  $A = 1$ ,  $B = 2$ ,  $C = 3$ ,  $D = 4$ , and  $E = 5$ . Assume we want to send a message of length 3. Recover the lost part of the message, or explain why it can not be done.

1. C\_AA

2. CE\_ \_

2. Suppose we want to send  $n$  packets, and we know  $p = 20\%$  of the packets will be erased. How many extra packets should we send? What happens if  $p$  increases (say to 90%)?