Cryptography

43. There are many instances when people might want to conceal information, or at least write it in some code that other people cannot read. We might be sending our credit card number via the internet to buy something, or transmitting confidential information to a business partner. Spies and terrorists also have an obvious need to transmit information that cannot be understood by others.

Coding and decoding messages is known as cryptography. In this, mathematics can be very useful (to all these people — there is nothing to stop it being used for bad purposes as much as for good). In fact, some well known mathematicians worked at Bletchley Park in World War II, breaking Nazi codes, an effort which undoubtedly changed the course of the war. Nowadays, the U.S. National Security Agency is said to be the world's largest single employer of mathematicians (several hundreds are said to work there).

44. One of the simplest codes was supposedly invented or used by Julius Caesar. If the message is "Meet me in Zabbar." we simply replace each 'a' by 'b', 'b' by 'c', 'c' by 'd', and so on, resulting in "Nffu nf jo Abccas". We have shifted each letter up one place; the person receiving the message then shifts each letter *down* by one place to get the original message.

Another variant is to shift each letter up by k places, for some fixed k. If we take $k = 3$, we would get "Phhw ph lq Cdeedu." However, anyone who intercepts such a message can decode it fairly easily, even if they don't know what value of k was used. Exercise: Try to decode this message — "Ymnx nx xnruqj."

There is a more sophisticated version, which is basically what is used by many governments and businesses around the world today. In this version, each letter is shifted by a different amount (say, the first letter is shifted 7 places, the next one 1 places, the next one 4 places, etc.). These values $(7, 1, 4, \ldots)$ are called the key. Anyone who knows the key can encode *and decode* messages, and it is therefore essential that the key be kept private. So if a business was communicating with different clients, it would have a separate key for each client, so that none of them could decode each other's messages. These sorts of schemes are known as private key cryptography.

45. There are several occasions where private key cryptography is impractical. On the internet, when customers want to send their credit card numbers to a company, they have no secure way of communicating with the company to agree the shifts (if they did have such a secure way, there would be no

need for cryptography in the first place). Similarly, spies may live for years without any direct contact with their spy masters.

These situations led to the development of Public Key Cryptography. In this system, the company provides a public key that everyone can use to encode the messages that they want to send to the company. However, this public key is of little or no use when it comes to decoding the messages. For that, a second, private, key is needed, and that is known only to the company. So all the customers encode their messages (e.g. their credit card numbers) with the public key, but only the company can decode them, because only it has the second key.

46. Here is one example of Public Key Cryptography (due to Neal Koblitz)[4]. The company (Best Products Inc.) chooses two integers a and b, sets $M = ab-1$, then chooses two more integers a' and b', and finally sets $e = a'M+a$, $d = b'M+b$, and $n = (ed-1)/M = a'b'M + ab' + a'b + 1$. The public key is the values of n and e, and the private key is d. (The letter "e" was chosen to signify "encryption" and "d" to signify "decryption.") To send Best Products some number m ("m" for "message"), so long as $m < n$, one computes $c = em \pmod{\text{n}}$. The value of "c" is what is actually "communicated" to the company. Best Products then deciphers this by calculating $dc \pmod{\text{n}}$.

Note that $de = Mn + 1 \equiv 1 \pmod{\text{n}}$, and therefore $dc = d(em) = (de)m \equiv m \pmod{\text{n}}$. So calculating $dc \pmod{\text{n}}$ does tell Best Products what the original message m was.

47. Let us work out an example. We will choose $a = 11$, $b = 13$, $a' = 17$, $b' = 23$. Then

$$\begin{aligned} M &= ab-1 &&= (11 \times 13) - 1 = 142 \\ e &= a'M + a &&= (17 \times 142) + 11 = 2425 \\ d &= b'M + b &&= (23 \times 142) + 13 = 3279 \\ n &= (ed-1)/M &&= (2425 * 3279 - 1)/142 = 7,951,574/142 = 55,997 \end{aligned}$$

Best Products can tell all customers (and even publish on its website) the values of n and e. Now suppose that a customer wants to send BestProducts a "credit card number", say 1274; this is m. The customer calculates $c = em \pmod{\text{n}}$. Now $em = 2425 \times 1274 = 3,089,450$, and since $3,089,450 = (55,997 * 55) + 9615$ we have $em = 9615 \pmod{55997}$, so $c = 9615$.

[4]It uses modular arithmetic, which will actually be introduced in the next section. This is only because I am still re-writing the modular arithmetic notes — in future versions of these notes, modular arithmetic will be introduced before cryptography.

The customer therefore sends Best Products the number 9615. Anyone who happens to read this may would also know the (public) values of n and e, but it is not immediately clear how to obtain the value of m. However, Best Products knows the value of d, which it has kept private. It can then calculate $dc \pmod{\text{n}} = (3279 \times 9615) \pmod{55,997} = 31,527,585 \pmod{55,997} = 1274$.

48. I am grateful to Neal Koblitz for describing the system in 45, as well as the following scheme, at www.math.washington.edu/ koblitz/crlogia.html. You can actually skip these last three paragraphs if you want. I only included them because they seemed neat.

Information hiding is related to cryptography. Suppose a group of people wants to know how many cigarettes they smoke between them (or how much money they spend on gambling, or how much weight they gained at Christmas). They are all willing to help compile the statistics, but only if there is complete confidentiality; that is, no person wants their individual figure to be known. They can do this as follows.

Suppose the numbers are 9, 3, 7, 0, 2. The first person thinks of some large number (say 56412), adds his number of cigarettes ($56412 + 9 = 56421$) and whispers the answer to the next person. This person adds their number ($56421+3 = 56424$) and whispers this answer to the next person. The remaining people similarly work out $56424+7 = 56431$, $56431+0 = 56431$, $56431+2 = 56433$. The last person gives this answer to the first person, who subtracts the original large number, 56412, to get the total, 21.