Bonus Lesson: Cryptography

Attila wants to send Brigi a message so that only she can read it. To do so, Attila and Brigi first decide on a ***cryptosystem***, a suite of algorithms for coding and decoding messages. Attila uses the ***cipher*** together with the ***encryption key*** to ***encrypt*** his message. His ***plaintext*** message which was readable by anyone now appears as unintelligible ***ciphertext***, which he sends to Brigi. Brigi uses the ***decryption key*** to ***decrypt*** the ciphertext, recovering the original plaintext message.

1 Basic private key cryptosystems

Politics

1.1 In certain computer bulletin-board systems it is customary, if you want to post a message that may offend some people (e.g., a dirty joke), to encipher the letters (but not the blanks or punctuation). It is then possible to decipher the text if one wants to, but no one is forced to see a message that jars on the nerves. Decipher the punchline of the following story:

> *At an international convention of surgeons, representatives of different countries were comparing notes on recent advances in reattaching severed parts of the body. The French, Americans and Russians were being especially boastful. The French surgeon said, "We sewed a leg on an injured runner, and a year later he placed in a national 1000-meter race." "Using the most advanced surgical procedures," the Russian surgeon chimed in, "we were able to put back an athlete's entire arm, and a year later with the same arm he established a new world record for the shot put." But they all fell silent when the American, not to be outdone, announced that* ***"Jr frjrq n fzvyr ba n ubefr'f nff, naq n lrne yngre vg jnf ryrpgrq Cerfvqrag!"***[1]

Caesar cryptosystem Attila wishes to send Brigi a word W comprised of letters from the 26 letter English alphabet.

i. Attila and Brigi agree privately on a letter, say D, which serves as the encryption and decryption key.

ii. Attila changes every letter in the plaintext word W according to the table below to generate the ciphertext word $\widetilde{W}$.

A	B	C	D	E	F	G	H	···	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	···	V	W	X	Y	Z	A	B	C

The first row of this table is the alphabet, in order. The second row is the shifted alphabet, beginning with the chosen letter and transitioning from Z to A.

iii. Brigi uses the table in reverse to change every letter in $\widetilde{W}$ to recover the original word W.

Example: The plaintext word RATIONAL in the Caesar cryptosystem with key letter D becomes the ciphertext UDWLRQDO.

Practice

1.2 The five most frequently used letters in the English alphabet are, in order, E, T, A, O, and I. Using this information, explain how you might crack a Caesar cipher.

1.3 The following quotation is attributed to a famous mathematician:

GSGZNKSGZOIGRVXUHRKSYNUARJHKJOLLOIARZOTUXJKXZUKTZOIK

AYEKZTUZIUSVRKZKREOTGIIKYYOHRKRKYZOZSUIQGZUAXKLLUXZYJGBOJNORHKXZ

[1] This exercise was taken nearly verbatim from Neal Koblitz's *A course in Number Theory and Cryptography*, second edition, published ***1994***. The story is meant as a number theory exercise, not as commentary on any current or future political figure.

It seems that all punctuation has been removed. Assuming the message was encrypted used a Caesar cipher, use frequency analysis to help decrypt the message.

1.4 Associating A with 0, B with 1, C with 2, ..., Y with 24, and Z with 25, describe the Caesar cryptosystem using modular arithmetic. What form does the encryption and decryption key take, and how are encryption and decryption performed?

In a ***private key cryptosystem***, knowledge of the encryption and decryption keys is private, shared only between the users of the system. The Caesar cryptosystem is a private key cryptosystem. Such systems work well when the users can securely communicate and agree on the keys with one another.

In the cryptosystems that follow, messages (plaintext and ciphertext) will consists of positive integers instead of words from the English alphabet. It is still possible to encrypt text: transforming a message written in English into a positive integer can be done in a number of ways. (Can you come up with a way to do this?) The users of any cryptosystem can agree publicly or privately on the mapping between English text and the positive integers.

Affine cryptosystem Attila wishes to send Brigi a number N.

i. Attila and Brigi agree privately on integers a, b, c, and m where $ac \equiv 1 \pmod{m}$.

ii. Attila computes the ciphertext $\widetilde{N} = aN + b$ and sends it to Brigi.

iii. Brigi recovers the modulo m residue of the plaintext N by computing $c(\widetilde{N} - b)$.

All computations are done modulo m.

Example: Attila and Brigi agree on $a = 191$, $b = 45$, $c = 1754$, and $m = 335013$. Using the affine cryptosystem, they can send encrypted integers between 0 and 335012 to each other. If Attila's plaintext message is $N = 211518$, he computes $aN + b = 40399983 \equiv 198423 \pmod{m}$ and sends the ciphertext $\widetilde{N} = 198423$ to Brigi. Now Brigi computes $c(\widetilde{N} - b) = 347955012 \equiv 211518 \pmod{m}$, which is Attila's original plaintext message.

Practice

1.5 Use an affine cryptosystem with $m = 1000000$ to send your birthdate to a partner in the format ddmmyy.

1.6 Explain the Caesar cryptosystem as a special case of the affine cryptosystem. What values do the parameters take?

1.7 Explain why Brigi obtains Attila's original message, that is, explain why this cryptosystem works.

1.8 You've been hired by the Justice League to crack the zip code encryption used by the Evil Realtor's Association. You know they use an affine cryptosystem with $m = 100000$ to encrypt 5 digit zip codes. Eavesdropping for several days, you hear the ciphertexts 84576 and 33154 most frequently. Market research reveals that the two hottest zip codes in America are 49508 (Kentwood, MI) and 80922 (Colorado Springs, CO). Crack the Evil Realtor's Association's zip code encryption by determining the encryption key (a, b).

2 A "no key" cryptosystem and the discrete logarithm problem

In a ***"no key" cryptosystem***, the encryption and decryption keys are user-specific and are never communicated. This is useful when there is not a guaranteed secure way for users to communicate encryption and decryption keys with one another.

Massey-Omura cryptosystem Attila wishes to send Brigi a number N.

i. Attila and Brigi agree publicly on a large prime p. Attila privately chooses integers a and c such that $ac \equiv 1 \pmod{p-1}$, and Brigi privately chooses integers b and d such that $bd \equiv 1 \pmod{p-1}$.

ii. Attila computes $N_1 = N^a$ and sends it to Brigi.

iii. Brigi computes $N_2 = N_1^b$ and sends it to Attila.

iv. Attila computes $N_3 = N_2^c$ and sends it to Brigi.

v. Brigi recovers the modulo p residue of the plaintext N by computing N_3^d.

All computations are done modulo p.

Example: Attila wants to send Brigi his favorite two digit number $N = 58$. They decide to use $p = 101$. Attila privately selects $a = 13$ and $c = 77$, Brigi privately selects $b = 17$ and $d = 53$, and they do not share these numbers with anyone. Attila sends Brigi the least non-negative residue of the number 58^{13} modulo 101, which is 19. Brigi responds with $68 \equiv 19^{17} \pmod{101}$, then Attila responds with $79 \equiv 68^{77} \pmod{101}$. Finally, Brigi computes the least non-negative residue of 79^{53} modulo 101, which is Attila's favorite number 58.

Practice

2.1 Use the Massey-Omura cryptosystem with $p = 31$ to trade your favorite integer between 0 and 30 with a partner.

2.2 Explain why Brigi obtains Attila's original message, that is, explain why this cryptosystem works. *(Hint available.)*

The security of the Massey-Omura cryptosystem is based on the discrete logarithm problem. Let a, m, and r be integers. The ***discrete logarithm problem*** is to determine k such that $r^k \equiv a \pmod{m}$, if such a k even exists. In other words, the discrete logarithm problem is to determine "$\log_r a$ modulo m." While it is easy to compute the modulo m residue of any particular power of r, it is (as far as we can tell in the year 2020) extremely difficult to compute $\log_r a$. The asymmetry between the time it takes to compute exponents and logarithms modulo m is precisely what is exploited to make cryptosystems such as the Massey-Omura and ElGamal cryptosystems.

Example: The prime $p = 2^{521} - 1$ has 157 digits, and 3 is a primitive root modulo p. It takes only ≈ 130 multiplications of integers with at most 157 digits to compute the least non-negative residue of $3^{41567484613255311154}$ modulo p: it is

$$4902101596624595509475053110439120963997951094871249016012181112002935950464867442227728391131194363921492399359850674274694649788423989368020813189310176917$$

It is much, much more difficult, however, to find k such that 3^k is congruent to some given 157 digit number. Because 3 is a primitive root, there are $p - 1$ many possibilities for k, and listing them all out is computationally infeasible for extremely large values of p.

Cryptoanalysis

2.3 An eavesdropper on the Massey-Omura cryptosystem learns the residues of N^a, N^b, and N^{ab} modulo p. Show that if the eavesdropper can compute discrete logarithms, then he can recover the plaintext N. *(Hint available.)*

3 A public key cryptosystem based on the discrete logarithm problem

In a ***public key cryptosystem***, the encryption key is public knowledge while the decryption key is known only to a single user. In such a system, anyone can encrypt messages, but only one user can decrypt them.

Public key cryptosystems are useful when there is not a guaranteed secure way for users to privately communicate encryption and decryption keys with one another.

ElGamal cryptosystem Attila wishes to send Brigi a number N.

i. Attila and Brigi agree publicly on a large prime p and a primitive root r modulo p. Brigi privately chooses an integer b between 0 and $p-1$ and makes public the encryption key $e = r^b$.

ii. Attila privately chooses an integer a, computes $\tilde{r} = r^a$ and $\widetilde{N} = Ne^a$, and sends $\tilde{r}$ and $\widetilde{N}$ to Brigi.

iii. Brigi recovers the modulo p residue of the plaintext N by computing $\widetilde{N}\tilde{r}^{p-1-b}$.

All computations are done modulo p.

Example: Attila wants to send Brigi his favorite two digit number $N = 58$. They decide to use $p = 101$ and the modulo 101 primitive root $r = 12$. Brigi privately chooses $b = 27$ and publishes the encryption key $e = 75$, the least non-negative residue of 12^{27} modulo 101. Attila privates chooses $a = 71$ and sends Brigi the ciphertext $\tilde{r} = 72 \equiv 12^{71} \pmod{101}$ and $\widetilde{N} = 51 \equiv 58 \cdot 75^{71} \pmod{101}$. Now Brigi recovers the Attila's favorite two digit number by finding the least non-negative residue of $51 \cdot 72^{101-1-27}$ modulo 101, which indeed is 58.

Practice

3.1 Use the ElGamal cryptosystem with $p = 31$ to trade the day of the month (minus 1) of your birthday with a partner.

3.2 Explain why Brigi obtains Attila's original message, that is, explain why this cryptosystem works. *(Hint available.)*

The security of the ElGamal cryptosystem is based on the ***Diffie-Hellman assumption*** which states that, with knowledge only of r, r^a, and r^b modulo p, it is computationally infeasible to determine the modulo p residue of r^{ab}. This is closely related to the discrete logarithm problem but to date has not been shown to be equivalent.

Cryptoanalysis

3.3 An eavesdropper on the ElGamal cryptosystem has knowledge of the modulo p residues of r, r^a, r^b, and Nr^{ab}. Show that if the eavesdropper knows how to invalidate the Diffie-Hellman assumption, then he can recover the modulo p residue of the plaintext N.

3.4 Show that under the Diffie-Hellman assumption, the ElGamal cryptosystem is secure. More precisely, show that if one knows how to crack the ElGamal cryptosystem (that is, recover N from knowledge of the modulo p residues of r, r^a, r^b, and Nr^{ab}), then one can render the Diffie-Hellman assumption incorrect.

3.5 Show that a solution to the discrete logarithm problem – that is, an ability to compute discrete logarithms efficiently – yields the Diffie-Hellman assumption incorrect. (It is conjectured, but not proven, that the Diffie-Hellman assumption and the discrete logarithm problem are equivalent.)

3.6 Show that if one knows how to crack the ElGamal cryptosystem (that is, recover N from knowledge of the modulo p residues of r, r^a, r^b, and Nr^{ab}) then one knows how to crack the Massey-Omura cryptosystem (that is, recover r from knowledge of the modulo p residues of r^a, r^b, and r^{ab}). *(Hint available.)*

4 A public key cryptosystem based on factorization

The problem of determining the prime factorization of an integer is called the ***factorization problem***. To the best of our knowledge in the year 2020, the factorization problem is a difficult one, especially when compared to the inverse problem of finding the product of a set of integers. The asymmetry between the difficulty of multiplying and factoring can be exploited to make a public key cryptosystem such as the RSA cryptosystem.

Rivest-Shamir-Adleman (RSA) cryptosystem Attila wishes to send Brigi a number N.

i. Brigi privately chooses large primes p and q and integers b and d such that $bd \equiv 1 \pmod{(p-1)(q-1)}$. She makes public the modulus $m = pq$ and the encryption key b.

ii. Attila computes the ciphertext $\widetilde{N} = N^b$ and sends it to Brigi.

iii. Brigi recovers the modulo m residue of the plaintext N by computing $\widetilde{N}^d$.

All computations are done modulo m.

Example: Attila would like to send Brigi his 7 digit phone number, $N = 3320402$. Brigi selects $p = 3041$, $q = 3307$, $b = 9764357$, and $d = 3438413$. She publishes the modulus $m = 10056587$ and the encryption key b. Attila computes the ciphertext $\widetilde{N} = 6090292 \equiv 3320402^{9764357} \pmod{m}$ and sends it to Brigi. Brigi recovers Attila's phone number by computing the least non-negative residue of $\widetilde{N}^{3438413}$, which is indeed 3320402.

Practice

4.1 Use RSA encryption to share your phone's area code with a partner. (If it helps, considering selecting primes from this list: 19, 23, 29, 31, 37, 41, 43, 47, 53.)

4.2 Assuming the extended version of Fermat's little theorem below, explain why Brigi obtains Attila's original message, that is, explain why this cryptosystem works.

4.3 An eavesdropper on the RSA cryptosystem learns of b and the modulo m residue of N^b. Show that if the eavesdropper has a solution to the factorization problem, then he can crack the RSA cryptosystem (that is, recover the plaintext N).

4.4 A cryptography message board calls for users to submit their favorite three digit number using the modulus 1387 and encryption key 121. User LEET, whom you don't particularly like, submits the cyphertext 596. Determine LEET's favorite three digit number and use it to explain why you don't particularly like LEET.

Fermat's little theorem, extended If m is squarefree and $k \equiv 1 \pmod{\varphi(m)}$, then $a^k \equiv a \pmod{m}$.

Example: The number $595 = 5 \cdot 7 \cdot 17$ is squarefree, and $\varphi(595) = 384$. The extended version of Fermat's little theorem says, in particular, that $a^{385} \equiv a \pmod{595}$ for any integer a; for example, $5^{385} \equiv 5 \pmod{595}$. This example does not follow from Fermat's little theorem or the Euler-Fermat theorem because 595 is not prime and 5 and 595 are not relatively prime.

Through the proof

4.5 Put $m' = m/\gcd(a, m)$. Show that $a^k \equiv a \pmod{m'}$. *(Hint available.)*

4.6 Show that $a^k \equiv a \pmod{\gcd(a, m)}$.

4.7 Combine the previous two problems to deduce that $a^k \equiv a \pmod{m}$. *(Hint available.)*