Cryptography
Homework #1 Solutions
Fall 2018

(1) Decrypt the following codes. In each case do not simply give your answer. You must say what methods you used to solve the problem.

(a) Substitution cipher

WBYAYAGHQTWBJNJUYHHYHUGVWBJPJKRGHYHUWBYAYAGHQTWBJVYPAWA
YIWBJVYPAWVGPJWFAWJGVFNYWWJPKEICBYKBCYQQNJIPGVVJPJLWGEATJFPN
TTJFPEHQJAA,NTFAEIPJDJPJKGOJPTGVDGPFQBJFQWBFHLDFPWYFQOYUGP,CJFP
YAJFUFYHFHLWFRJGEPAWFHLVGPVPJJLGDFAYHWBJGQLJHWYDJ

Plain text

This is only the beginning of the reckoning. This is only the first sip, the first foretaste of a bitter cup which will be proffered to us year by year unless, by a supreme recovery of moral health and martial vigor, we arise again and take our stand for freedom as in the olden time.

(b) Affine cipher (mod 26)

IQTLKCFQMWTUICJRPUPWIQTLMLCJQTSBUJCFFIQTLBQJKPWOOQPTLWJQGLTCO
GURGQDWOYOTUOWWTLWJQGLTFWTYOOTJQDWUPTUBQPQOLTLWIUJAIWCJW
QPTUHQPRYZTLWPCTQUPOIUYPROTUMCJWBUJLQKILUOLCFFLCDWHUJPWTLW
HCTTFWCPRBUJLQOIQRUICPRLQOUJZLCPTURUCFFILQMLKCSCMLQWDWCPRML
WJQOLCVYOTCPRFCOTQPGZWCMWCKUPGUYJOWFDWOCPRIQTLCFFPCTQUPO

Plain text

With malice toward none; with charity for all; with firmness in the right, as God gives us to see the right, let us strive on to finish the work we are in; to bind up the nation's wounds; to care for him who shall have borne the battle, and for his widow, and his orphan--to do all which may achieve and cherish a just and lasting peace, among ourselves, and with all nations.

(2) (a) Use the Euclidean algorithm to compute gcd(245873646,765384)
(b) Find u,v such that $\mathbf{245873646}u + \mathbf{765384}v$ equals the gcd from (a).

gcd(245873646,765384)
245873646 = 321*765384 + 185382
765384 = 4*185382 + 23856
185382 = 7*23856 + 18390
23856 = 1*18390 + 5466
18390 = 3*5466 + 1992
5466 = 2*1992 + 1482
1992 = 1*1482 + 510
1482 = 2*510 + 462
510 = 1*462 + 48

462 = 9*48 + 30
48 = 1*30 + 18
30 = 1*18 + 12
18 = 1*12 + 6
12 = 2*6 + 0

Hence gcd(245873646,765384) = 6

(b)
6 = 18 – 12 = 18 – (30 – 18) = 2*18 – 30 = 2*(48 – 30) – 30 =2*48 – 3*30 = 2*48 – 3*(462 – 9*48)
= 29*48 – 3*462 = 29*(510 – 462) – 3*462 = 29*510 – 32*462 = 29*510 - 32*(1482 – 2*510)
= 93*510 - 32*1482 = 93*(1992 – 1482) +- 32*1482 = 93*1992 – 125*1482
= 93*1992 – 125*(5466 – 2*1992) = 343*1992 – 125*5466 = 343*(18390 – 3*5466) – 125*5466
= 343*18390 – 1154*5466 = 343*18390 – 1154*(23856 - 18390) = 1497*18390 – 1154*23856
= 1497*(185382 – 7*23856) - 1154*23856 = 1497*185382 – 11633*23856
= 1497*185382 – 11633*(765384 – 4*185382) = 48029*185382 – 11633*765384
= 48029*(245873646 - 321*765384) – 11633*765384 = **48029*245873646 – 15428942*765384**

(3) Suppose that $a_1 \equiv a_2 \pmod{m}$, $b_1 \equiv b_2 \pmod{m}$. Prove that
$a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$, $a_1 b_1 \equiv a_2 b_2 \pmod{m}$

Proof:
$a_1 \equiv a_2 \pmod{m}, b_1 \equiv b_2 \pmod{m} \Rightarrow a_1 = a_2 + k_1 m,\ b_1 = b_2 + k_2 m$
$a_1 + b_1 = a_2 + k_1 m + b_2 + k_2 m = (a_2 + b_2) + (k_1 + k_2)m \Rightarrow a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$
$a_1 b_1 = (a_2 + k_1 m)(b_2 + k_2 m) = a_2 b_2 + (a_2 k_2 + b_2 k_1 + k_1 k_2 m)m \Rightarrow a_1 b_1 \equiv a_2 b_2 \pmod{m}$

(4) Write a multiplication table for $(Z/9Z)^*$, Note the number of units in $Z/9Z$ is

$$\phi(9) = 9 * \left(1 - \frac{1}{9}\right) = 6$$

*	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

(5) Compute the following modular operations. Show intermediate steps as appropriate.
(a) $2846 * 7645 \pmod{353}$
(b) $367^7 \pmod{503}$
(c) $11^{507} \pmod{1237}$

(a) $2846 \equiv 32 \pmod{353}, 7645 \equiv 232 \pmod{353} \Rightarrow 2846 * 7645 \equiv 11 \pmod{353}$

(b)

$7 = 4 + 2 + 1$

$367^1 \equiv 367 \pmod{503}$, $367^2 \equiv 388 \pmod{503}$, $367^4 \equiv 388^2 \equiv 147 \pmod{503}$

$367^7 \equiv 367 * 388 * 147 \equiv 370 \pmod{503}$

(c)

$507 = 256 + 128 + 64 + 32 + 16 + 8 + 2 + 1$

$11^1 \equiv 1 \pmod{1237}$, $11^2 \equiv 121 \pmod{1237}$, $11^4 \equiv 121^2 \equiv 1034 \pmod{1237}$

$11^8 \equiv 1034^2 \equiv 388 \pmod{1237}$, $11^{16} \equiv 388^2 \equiv 867 \pmod{1237}$, $11^{32} \equiv 867^2 \equiv 830 \pmod{1237}$

$11^{64} \equiv 830^2 \equiv 1128 \pmod{1237}$, $11^{128} \equiv 1128^2 \equiv 748 \pmod{1237}$, $11^{256} \equiv 748^2 \equiv 380 \pmod{1237}$

$11^{507} \equiv 11 * 121 * 388 * 867 * 830 * 1128 * 748 * 380 \equiv 322 \pmod{1237}$

(6) Find all solutions for x in the range $0,\ldots,m-1$ for the following

(a) $4x \equiv 3 \pmod{13}$

(b) $x^2 \equiv 2 \pmod{13}$

(c) $x^2 \equiv 3 \pmod{13}$

(a) $4x \equiv 3 \pmod{13}$ has a solution $x = 4$

(b) $x^2 \equiv 2 \pmod{13}$ has no solutions

(c) $x^2 \equiv 3 \pmod{13}$ has solutions $x = 4, x = 9$

(7) Compute the following numbers a compute $a^{-1} \pmod{p}$ two ways: using the extended Euclidean Algorithm and using Fermat's Little Theorem

(a) $9^{-1} \pmod{11}$

(b) $1001^{-1} \pmod{12347}$

(a) Extended Euclidean method. First compute gcd(9,11)

$11 = 9 + 2$

$9 = 4 * 2 + 1$

$1 = 9 - 4 * 2 = 9 - 4 * (11 - 9) = 5 * 9 - 4 * 11 \Rightarrow$

$9^{-1} \equiv 5 \pmod{11}$

Fermat's Little Theorem shows that

$9^{10} \equiv 1 \pmod{11} \Rightarrow 9^{-1} \equiv 9^9 \pmod{11}$

$9 = 8 + 1$

$9^1 \equiv 9 \pmod{11}$, $9^2 \equiv 81 \equiv 4 \pmod{11}$, $9^4 \equiv 4^2 \equiv 16 \pmod{11}$, $9^8 \equiv 16^2 \equiv 256 \equiv 3 \pmod{11}$

$9^{-1} \equiv 9^9 \equiv 9 * 3 \equiv 5 \pmod{11}$

(b) Extended Euclidean method. First compute gcd(1001,12347)

$$12347 = 12*1001 + 335$$
$$1001 = 2*335 + 331$$
$$335 = 1*331 + 4$$
$$331 = 82*4 + 3$$
$$4 = 1*3 + 1$$
$$1 = 4 - 3 = 4 - (331 - 82*4) = 83*4 - 331 = 83*(335 - 331) - 331 = 83*335 - 84*331$$
$$= 83*335 - 84*(1001 - 2*335) = 251*335 - 84*1001 = 251*(12347 - 12*1001) - 84*1001$$
$$= 251*12347 - 3096*1001 \Rightarrow$$
$$1001^{-1} \equiv -3096 \equiv 9251 \pmod{12347}$$

Fermat's Last Theorem shows (12347 is prime)

$$1001^{12346} \equiv 1 \pmod{12347} \Rightarrow 1001^{-1} \equiv 1001^{12345} \pmod{12347}$$
$$12345 = 8192 + 4096 + 32 + 16 + 8 + 1$$
$$1001^{1} \equiv 1001 \pmod{12347},\ 1001^{2} \equiv 1894 \pmod{12347},\ 1001^{4} \equiv 1894^{2} \equiv 6606 \pmod{12347},$$
$$1001^{8} \equiv 6606^{2} \equiv 4938 \pmod{12347},\ 1001^{16} \equiv 4938^{2} \equiv 10866 \pmod{12347},\ 1001^{32} \equiv 10866^{2} \equiv 7942 \pmod{12347},$$
$$1001^{64} \equiv 7942^{2} \equiv 6888 \pmod{12347},\ 1001^{128} \equiv 6888^{2} \equiv 7370 \pmod{12347},$$
$$1001^{256} \equiv 7370^{2} \equiv 2447 \pmod{12347},\ 1001^{512} \equiv 2447^{2} \equiv 11861 \pmod{12347},$$
$$1001^{1024} \equiv 11861^{2} \equiv 1603 \pmod{12347},\ 1001^{2048} \equiv 1603^{2} \equiv 1433 \pmod{12347},$$
$$1001^{4096} \equiv 1433^{2} \equiv 3887 \pmod{12347},\ 1001^{8192} \equiv 3887^{2} \equiv 8388 \pmod{12347}$$
$$1001^{12345} \equiv 1001*4938*10866*7942*3887*8388 \equiv 9251 \pmod{12347}$$

(8) (a) Determine if 2 is a primitive root modulo 11.
(b) Determine if 2 is a primitive root modulo 23.
(c) Find all primitive roots modulo 11.

(a) 2 is a primitive root mod 11

$$p = 11,\ p - 1 = 10 = 2*5$$
$$(p-1)/2 = 5,\ (p-1)/5 = 2$$
$$a = 2$$
$$2^{5} \equiv 32 \equiv 10 \pmod{11},\ 2^{2} \equiv 4 \pmod{11}$$

(b) 2 is not a primitive root mod 23

$$p = 23,\ p - 1 = 22 = 2*11$$
$$(p-1)/2 = 11,\ (p-1)/11 = 2$$
$$a = 2$$
$$2^{11} \equiv 2048 \equiv 1 \pmod{23}$$

(c) $a = 2, 6, 7, 8$ are primitive roots mod 11

$a = 6$

$6^5 \equiv 10 \pmod{11},\ 6^2 \equiv 3 \pmod{11}$

$a = 7$

$7^5 \equiv 10 \pmod{11},\ 7^2 \equiv 5 \pmod{11}$

$a = 8$

$8^5 \equiv 10 \pmod{11},\ 8^2 \equiv 9 \pmod{11}$

$a = 3, 4, 5, 9, 10$ are **not** primitive roots mod 11

$a = 3$

$3^5 \equiv 1 \pmod{11}$

$a = 4$

$4^5 \equiv 1 \pmod{11}$

$a = 5$

$5^5 \equiv 1 \pmod{11}$

$a = 9$

$9^5 \equiv 1 \pmod{11}$

$a = 10$

$10^2 \equiv 1 \pmod{11}$

(9) Consider Vernam's cipher: $c(m) = k \oplus m,\ d(c) = k \oplus c$ (where k is the secret key).
(a) Explain why this cipher is vulnerable to a plaintext attack.
(b) If $c = 1011001001010110$ and $m = 0011101100010001$ use your attack method in (a) to find the secret key k.

(a) $c \oplus m = k \oplus m \oplus m = k \oplus 0 = k$ Hence we can always find the key k if m and c are both known.
(b) $k = c \oplus m = 1011001001010110 \oplus 0011101100010001 = 1000101101000111$

(10) Bob and Alice use a multiplication cipher $c = km$ (where the secret key k is a large prime). Eve intercepts two ciphertexts: $c_1 = 12849217045006222,\ c_2 = 6485880443666222$ Use gcd to find the secret key k.

$c_1 = 12849217045006222,\ c_2 = 6485880443666222$

$d = \gcd(c_1, c_2) = 174385766$

$d = 2 * 87192883 \Rightarrow k = 87192883$