Cryptography
Homework #1
Fall 2018

Due Monday, October 8

(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

(b) Affine cipher (mod 26)
IQTLKCFQMWTUICJRPUPWIQTLMLCJQTSBUJCFFIQTLBQJKPWOOQPTLWJQGLTCO
GURGQDWOYOTUOWWTLWJQGLTFWTYOOTJQDWUPTUBQPQOLTLWIUJAIWCJW
QPTUHQPRYZTLWPCTQUPOIUYPROTUMCJWBUJLQKILUOLCFFLCDWHUJPWTLW
HCTTFWCPRBUJLQOIQRUICPRLQOUJZLCPTURUCFFILQMLKCSCMLQWDWCPRML
WJQOLCVYOTCPRFCOTQPGZWCMWCKUPGUYJOWFDWOCPRIQTLCFFPCTQUPO

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

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

(4) Write a multiplication table for $(Z/9Z)^*$

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

(6) Find all solutions for *x* in the range 0,…,*m*-1 for the following
(a) $4x \equiv 3 \pmod{13}$
(b) $x^2 \equiv 2 \pmod{13}$
(c) $x^2 \equiv 3 \pmod{13}$

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

(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.

(9) Consider Vernam's cipher: $e(m) = k \oplus m,\ d(c) = k \oplus c$ (where k is the secret key).

(a) Explain why this cipher is vulnerable to a plaintext attck.

(b) If $c = 1011001001010110$ and $m = 0011101100010001$ use your attack method in (a) to find the secret key k.

(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.