

Name:

Math 424: Exam 3

1. (12 pts) An affine cipher has encryption function $5x - 1 \pmod{26}$. Compute the decryption function.

Solution: We use our egcd algorithm, obtaining the following table:

r_i	q	s_i	t_i
26	—	1	0
5	5	0	1
1	—	1	−5

Since $\gcd(5, 26) = 1$, I stop at the third row. We have $1 \cdot 26 - 5 \cdot 5 = 1$, so $(-5) \cdot 5 \equiv 1 \pmod{26}$. Also, $-5 \equiv 21 \pmod{26}$. Thus the inverse of 5 is 21. The decryption function is therefore

$$21(x + 1) \pmod{26}.$$

2. (12 pts) Convert the decimal number 19 to binary.

Solution: The table looks like this:

n	b
19	1
9	1
4	0
2	0
1	1

Therefore $19 = (10011)_2$.

3. (12 pts) The ciphertext 0110101 was encrypted with the one-time pad with key 1110011. What was the plaintext?

Solution: 10001110

4. (12 pts) A coin is flipped three times in a row. Given that the number of heads that came up was *even*, what is the probability that the flips were all tails?

Solution: One can just enumerate all possibilities: TTT, HHT, HTH, THH. Immediately we get $\frac{1}{4}$. Alternatively we can use the formula: Let A be the event that there are an even number of heads, and B the event that there are all tails. Clearly $A \cap B = B$, and $P(B) = \frac{1}{8}$. For A , since there are 3 flips, if there are an even number of heads, then there are an odd number of tails, and vice versa. Thus either there is an even number of heads, or an even number of tails, but not both. Since the two are mutually exclusive and equally likely, $P(A) = \frac{1}{2}$. Finally,

$$P(B | A) = \frac{P(A \cap B)}{P(A)} = \frac{1/8}{1/2} = \frac{1}{4}.$$

5. (12 pts) Given a cryptographic protocol, define what it means for the protocol to have *perfect secrecy*.

Solution: $\forall m$ in the messagespace, $\forall c$ in the cipherspace,

$$P(M = m \mid C = c) = P(M = m).$$