

Name:

Math 424: Exam 4

1. (15 pts) Suppose $G : \{0, 1\}^2 \rightarrow \{0, 1\}^6$ is a PRNG. Let E be the associated cryptosystem adapted from the one-time pad. What are the messagespace $\mathcal{M}$, cipherspace $\mathcal{C}$, and keyspace $\mathcal{K}$ for E ?

Solution: $\mathcal{M} = \mathcal{C} = \{0, 1\}^6$, $\mathcal{K} = \{0, 1\}^2$

2. (15 pts) Bob encrypts with a Caesar cipher. Eve plays the CI game with Bob. Give Eve's best first move and give her win probability. ("Best" means shortest with highest win probability; the move need not be unique.) No proof is required.

Solution: One answer is $m_0 = \text{"AA"}$ and $m_1 = \text{"AB"}$. The win probability is 100%.

Any pair of two-letter strings, where the distance between the pairs of letters is different, will work. In this case, the distance between the letters in m_0 is 0, and the distance in m_1 is 1. This distance is preserved under Caesar shift.

3. (15 pts) Compute the remainder when we divide 7^{17} by 23.

Solution: We have $17 = 1 + 16$. Computing powers of 7, we have

$$7^1 \equiv 7 \pmod{23}$$

$$7^2 = 49 \equiv 3 \pmod{23}$$

$$7^4 \equiv 3^2 \equiv 9 \pmod{23}$$

$$7^8 \equiv 9^2 \equiv 12 \pmod{23}$$

$$7^{16} \equiv 12^2 \equiv 6 \pmod{23}.$$

Therefore $7^{17} \equiv 7 \cdot 6 \equiv 19 \pmod{23}$.

4. (15 pts) Find the smallest nonnegative $x \in \mathbb{Z}$ satisfying the pair of congruences

$$x \equiv 2 \pmod{23} \text{ and } x \equiv 5 \pmod{37}.$$

Solution: We have $23 \cdot 37 = 851$. By Extended Euclidean algorithm, $-8 \cdot 23 + 5 \cdot 37 = 1$. Thus our solution is

$$5 \cdot -8 \cdot 23 + 2 \cdot 5 \cdot 37 \equiv 301 \pmod{851}.$$