**MATH/CMSC 456 (Washington) Final Exam Solutions Spring 2017**

**1.** (10 points) The encryption function is $Ax + B$. Choose $x = 0$ to get $B$ and $x = 1$ to get $A + B$. Subtract $B$ to get $A$.

**2.** (10 points) $n = 1$ yields $1 \equiv c_0 \cdot 0 + c_1 \cdot 1 + 2$, so $c_1 \equiv -1$.
$n = 2$ yields $0 \equiv c_0 \cdot 1 + c_1 \cdot 1 + 2$, so $c_1 \equiv -1$.

**3.** (10 points) The Basic Factorization Principle tells us that $\gcd(1208 - 1, 2201)$ is a non-trivial factor of 2201. Use the Euclidean Algorithm:

$$2201 = 1 \cdot 1207 + 994,\ 1207 = 1 \cdot 994 + 213,\ 994 = 4 \cdot 213 + 142, 213 = 1 \cdot 142 + 71,\ 142 = 2 \cdot 71 + 0.$$

The gcd is 71. The factorization is $2201 = 71 \times 31$.

**4.** (10 points) Eve makes two lists: (1) $E_K(m_1)$ for all $10^{10}$ keys $K$. (2) $c_1 \oplus B$ for all $10^{10}$ binary strings $B$. She finds all pairs $(K, B)$ that yield matches. She tests each such pair on the remaining $(m_i, c_i)$. It is very likely that only one key pair $(K, B)$ survives.

**5.** (a) (5 points) The ciphertext will be 5 letters repeated 60 times.
(b) (5 points) There will be no matches for displacements of 1, 2, 3, 4, 6. There will be 300 matches for displacement of 5.

**6.** (10 points) Since the first two letters of $c$ are the same, and the first two letters of *HELLO* are different, *HELLO* cannot encrypt to $c$, so the probability is 0. If there is perfect secrecy, the conditional probability must equal $\text{Prob}(m = HELLO)$, which it does not.

**7.** (10 points) There are $r = 10^5$ "people" and $N = 10^8$ "birthdays." The probability of a match is approximately $1 - e^{-r^2/2N} = 1 - e^{-50} \approx 1$. It is therefore very likely that there is a match.

**8.** (a) (5 points) The first shift is by 0 or 1. Therefore, the 4th shift is by 0 or 1. Since $I$ unshifts by 0 or 1 to $I$ or $H$, the message must be *YOUHAVEPASSED*.
(b) (5 points) Encrypt the two possibilities and see which one yields the ciphertext.
(c) (5 points) Add 100 random bits at the end of the message before encrypting.

**9.** (10 points) We need to solve $de \equiv 1 \pmod{(p-1)(q-1)}$, which means $7d \equiv 1 \pmod{192}$. Use the Extended Euclidean Algorithm to obtain $1 = 192(-2) + 7(55)$. Therefore, $d = 55$.

**10.** (a) (5 points) 4. Victor chooses $i = 1$ or $i = 2$ and asks Peggy for $R_i$, which she sends. 5. Victor checks that $2R_i = H_i$.
(b) (5 points) 1. Peggy chooses random $r_1$ mod $n$ and computes $r_2 \equiv x/r_1 \pmod{n}$.
2. Peggy computes $h_1 = r_1^2$ and $h_2 = r_2^2$ mod $n$ and sends $h_1$ and $h_2$ to Victor.
3. Victor checks that $h_1 h_2 \equiv s \pmod{n}$.
4. Victor chooses $i = 1$ or $i = 2$ and asks for $r_i$, which Peggy sends.
5. Victor checks that $h_i \equiv r_i^2$.
6. They repeat several times.

**11.** (10 points) It is fast. It is not collision-free: $h(M||M||M) = h(M)$. It is not preimage resistant: $h(M) = M$.

**12.** (a) (10 points) $N = p - 1$ since it deals with the exponents. Verification congruence:

$$r^r \equiv g^{kr} \pmod{p}, \quad h^m g^s \equiv g^{ma} g^{kr-am} \equiv g^{kr} \pmod{p}.$$

(b) (5 points) Eve needs to solve $5^5 h^{-m} \equiv g^s \pmod{p}$ for $s$. This is a discrete log problem, so it's hard.
(c) (5 points) Signing congruences: $r \equiv g^k \pmod{p}$ and $s \equiv kr - aH(m) \pmod{p-1}$; Verification: $r^r \equiv h^{H(m)} g^s \pmod{p}$.

**13.** (a) (7 points) $H$ is collision free, so if $H(\text{answer}) = H(\pi)$, we expect that answer $= \pi$.
(b) (3 points) The hash function should give random-looking binary strings, so about half of the binary digits should agree with the correct hash value and half should not. Therefore, the average should be approximately 50%.

**14.** (5 points) *HAVEAGOODSUMMER*

**MATH/CMSC 456 (Washington) Final Exam Solutions Spring 2017**

**1.** (a) (5 points) The first shift is by 1 or 2. Therefore, the 4th shift is by 1 or 2. Since $J$ unshifts by 1 or 2 to $I$ or $H$, the message must be *YOUHAVEPASSED*.
(b) (5 points) Encrypt the two possibilities and see which one yields the ciphertext.
(c) (5 points) Add 100 random bits at the end of the message before encrypting.
**2.** (10 points) The Basic Factorization Principle tells us that $\gcd(2256-1, 2501)$ is a non-trivial factor of 2501. Use the Euclidean Algorithm:

$$2501 = 1 \cdot 2255 + 246,\ 2255 = 9 \cdot 246 + 41,\ 246 = 6 \cdot 41 + 0.$$

The gcd is 41. The factorization is $2501 = 61 \times 41$.

**3.** (10 points) The encryption function is $Ax+B$. Choose $x=0$ to get $B$ and $x=1$ to get $A+B$. Subtract $B$ to get $A$.
**4.** (10 points) $n=1$ yields $2 \equiv c_0 \cdot 1 + c_1 \cdot 0 + 1$, so $c_1 \equiv 1$.
$n=2$ yields $0 \equiv c_0 \cdot 0 + c_1 \cdot 2 + 1$, so $c_1 \equiv 1$.
**5.** (a) (5 points) The ciphertext will be 4 letters repeated 100 times.
(b) (5 points) There will be no matches for displacements of 1, 2, 3, 5, 6. There will be 400 matches for displacement of 4.
**6.** (a) (7 points) $H$ is collision free, so if $H(\text{answer}) = H(\pi)$, we expect that answer $=\pi$.
(b) (3 points) The hash function should give random-looking binary strings, so about half of the binary digits should agree with the correct hash value and half should not. Therefore, the average should be approximately 50%.
**7.** (10 points) Since the first two letters of $c$ are the same, and the first two letters of *AFFINE* are different, *AFFINE* cannot encrypt to $c$, so the probability is 0. If there is perfect secrecy, the conditional probability must equal $\text{Prob}(m = AFFINE)$, which it does not.
**8.** (10 points) There are $r = 10^6$ "people" and $N = 10^9$ "birthdays." The probability of a match is approximately $1 - e^{-r^2/2N} = 1 - e^{-500} \approx 1$. It is therefore very likely that there is a match.
**9.** (a) (5 points) 4. Victor chooses $i=1$ or $i=2$ and asks Peggy for $R_i$, which she sends. 5. Victor checks that $2R_i = H_i$. (b) (5 points) 1. Peggy chooses random $r_1 \bmod n$ and computes $r_2 \equiv x/r_1 \pmod{n}$.
2. Peggy computes $h_1 = r_1^2$ and $h_2 = r_2^2 \bmod n$ and sends $h_1$ and $h_2$ to Victor.
3. Victor checks that $h_1 h_2 \equiv s \pmod{n}$.
4. Victor chooses $i=1$ or $i=2$ and asks for $r_i$, which Peggy sends.
5. Victor checks that $h_i \equiv r_i^2$.
6. They repeat several times.
**10.** (10 points) We need to solve $de \equiv 1 \pmod{(p-1)(q-1)}$, which means $11d \equiv 1 \pmod{216}$. Use the Extended Euclidean Algorithm to obtain $1 = 216(-3) + 11(59)$. Therefore, $d = 59$.
**11.** (10 points) It is fast. It is not collision-free: $h(M||M||M) = h(M)$. It is not preimage resistant: $h(M) = M$.
**12.** (a) (10 points) $N = p-1$ since it deals with the exponents. Verification congruence:

$$r^r \equiv g^{kr} \pmod{p}, \quad h^m g^s \equiv g^{ma} g^{kr-am} \equiv g^{kr} \pmod{p}.$$

(b) (5 points) Eve needs to solve $9^9 h^{-m} \equiv g^s \pmod{p}$ for $s$. This is a discrete log problem, so it's hard.
(c) (5 points) Signing congruences: $r \equiv g^k \pmod{p}$ and $s \equiv kr - aH(m) \pmod{p-1}$; Verification: $r^r \equiv h^{H(m)} g^s \pmod{p}$.
**13.** (10 points) Eve makes two lists: (1) $E_K(m_1)$ for all $10^{12}$ keys $K$. (2) $c_1 \oplus B$ for all $10^{12}$ binary strings $B$. She finds all pairs $(K, B)$ that yield matches. She tests each such pair on the remaining $(m_i, c_i)$. It is very likely that only one key pair $(K, B)$ survives.
**14.** (5 points) *HAVEAGOODSUMMER*