B

Department of Computer Science

Rochester Institute of Technology

CSCI–462 Introduction to Cryptography

Final Exam

May 2, 2018

Name: ....

Question 1 (6 points)

Compute the two public keys and the common key for the DHKE scheme with the parameters $p = 467$, $\alpha = 2$. Private keys are $a = 3$ and $b = 5$

- Alice's public key: ....
- Bob's public key: ....
- Common key: ....

Question 2 (2 points)

Assume a (small) company with 110 employees. A new security policy demands encrypted message exchange with a symmetric cipher. How many keys are required, if you are to ensure a secret communication for every possible pair of communicating parties?

Question 3 (4 points)

An RSA encryption scheme has the set-up parameters $p = 11$ and $q = 19$. The public key is $K_{Pub} = (n, e)$, where $e = 5$.

a) Compute the corresponding private key $K_{Pr} = (n, d)$. Use the extended Euclidean algorithm for the inversion and point out every calculation step.

a) Decrypt the ciphertext $y = 2$.

Question 4 (6 points)

Let E be an elliptic curve defined over $\mathbb{Z}_7$:

$$E : y^2 = x^3 + 3x + 2 \mod 7$$

For $P = (0, 3)$ calculate the point multiplication $3 \cdot P$ on E. Show the details of computations.

Question 5 (2 points)

Find the value of the Euler totient function $\phi(n)$ for $n = 444$.

Question 6 (6 points)

Hash functions. Let $X = \{0,1\}^m$ and $Y = \{0,1\}^n$ where m is much larger than n.

a) Explain what it means for a hash function $H : X \to Y$ to be one-way.

b) Explain what it means for a hash function $H : X \to Y$ to be collision resistant.

c) We consider a hash functions which produces output of lengths 128 bits ($n = 128$). After about how many random inputs do we have a probability at least 0.5 for a collision?

Question 7 (2 points)

What is the discrete logarithm problem?

Question 8 (3 points)

Give names of at least 3 well known hash functions. Which of those hash functions are considered secure?

Question 9 (2 points)

Why hash functions are typically a part of digital signature schemes?

Question 10 (2 points)

Briefly describe what the digital signatures are used for.

Question 11 (6 points)

Public-key cryptography.

a) What is the main difference between symmetric cryptography and public-key cryptography.

b) Why do we still use symmetric cryptography in current applications?

c) Give 3 examples of applications where public-key cryptography can be used.

Notes/Calculations