

APRIL 2014 Final Examination

FINAL EXAMINATION

Computer Science COMP-547B Cryptography and Data Security

15 APRIL 2014, 9h00

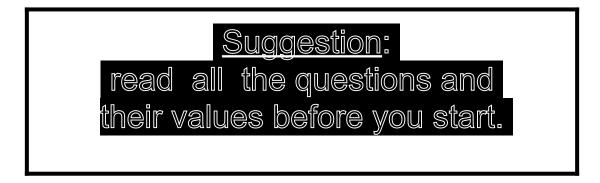
Examiner:	Prof. Claude Crépeau	Assoc Examiner:	Prof. David Avis
-----------	----------------------	--------------------	------------------

INSTRUCTIONS:

- This examination is worth 50% of your final grade.
- The total of all questions is 105 points.

• Each question heading contains (in parenthesis) a list of values for each sub-questions.

- This is an open book exam. All documentation is permitted.
- Faculty standard calculator permitted only.
- The exam consists of 6 questions on 3 pages, title page included.



Question 1. Perfect Elgammal? (10 +10 = 20 points)

Consider an Elgammal crypto-system with keys ($p, g, h=g^x \mod p, x$), where g generates all the non-zero elements mod p, except that only p,g are publicly available (but not h,x).

I) Explain how these public parameters may be generated efficiently.

Assume Alice and Bob use (h,x) as the secret encryption-decryption keys of an Elgammal crypto-system mod p for exactly one message m, 0<m<p.

II) Explain whether this one-time system is perfect or not.

Question 2. Hybrid Systems (10 + 10 = 20 points)

• Explain the purpose of a hybrid encryption scheme.

• Explain why we cannot combine a private-key MAC together with a digital signature scheme in a similar way to obtain hybrid authentication.

Question 3. Computational Assumptions (10 + 10 = 20 points)

a) Explain why the RSA assumption is potentially stronger than the factoring assumption and not the other way around.

b) Explain why the Diffie-Hellman assumption is potentially stronger than the Discrete Logarithm assumption and not the other way around.

Question 4. Number Theory vs Crypto (5 + 5 + 5 = 15 points)

For each of the following Number Theoretical concepts, name a Cryptographic concept which is related and explain the relation.

I) Euler's theorem.

2) Square root extraction modulo a prime.

3) Kalai's algorithm.

Question 5. DSS identification (10 points)

Elaborate a public-key identification scheme based on the DSS and justify the necessity of DSS being existentially unforgeable under chosen message attack to obtain a secure identification scheme.

Question 6. à la mode... (6 + 6 + 8 = 20 points)

What is the effect of a single-bit error in the ciphertext when using the CBC, OFB, and CTR modes of operation?

What is the effect of a dropped ciphertext block (i.e., if the ciphertext c_1, c_2, c_3, \ldots is received as c_1, c_3, \ldots) when using the CBC, OFB, and CTR modes of operation?

Say CBC-mode encryption is used with a block cipher having a 256-bit key and 128-bit block length to encrypt a 1024-bit message. What is the length of the resulting ciphertext?