McGill

APRIL 2017
Final Examination

FINAL EXAMINATION

Computer Science COMP-547
Cryptography and Data Security

20 APRIL 2017, 9h00-12h00

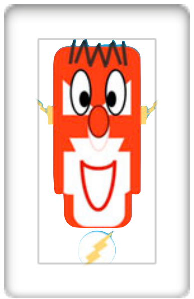
Examiner:	Prof. Claude Crépeau	Assoc Examiner:	Alice & Bob

INSTRUCTIONS:

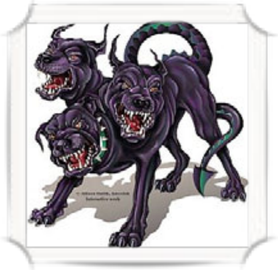
- This examination is worth 50% of your final grade.
- The total of all questions is 100 points.
- Each question heading contains (in parenthesis) a list of values for each sub-questions.
- This is an **open book** exam. **All documentation is permitted.**
- Faculty standard calculator permitted only.
- The exam consists of 5 questions on 3 pages, title page included.

Suggestion:
read all the questions and
their values before you start.

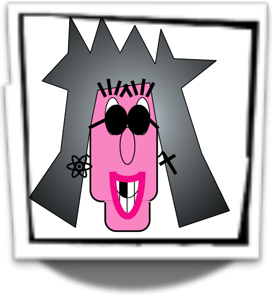
Question 1. Crypto-FACES ? (10+10 = 20 points)



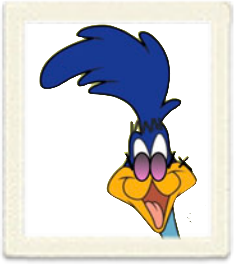
(A)



(B)

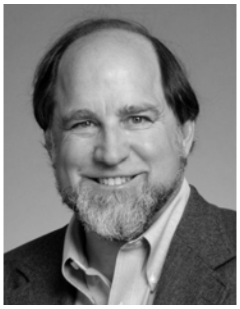


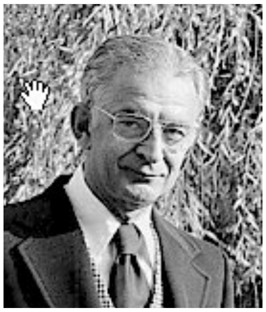
(C)

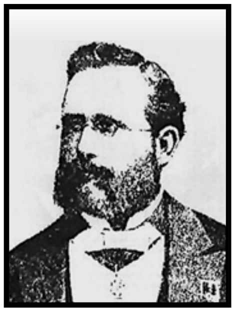


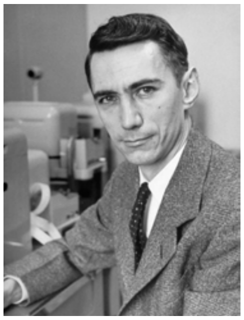
(D)

Identify each of the four characters above and explain some role they have played in cryptographic settings. Define some special attribute of each one of them.









Identify each of the four cryptographers above and explain some role they have played in the history of cryptography. For each one, explain one concept they have contributed.

Question 2. Pseudo-random permutation (10 + 10 = 20 points)

In general, every element in the domain of a permutation Π_k is part of a *cycle*. The length of the cycle containing $\mathbf{x}$ is the smallest integer $\mathbf{i} > 0$ such that $\Pi_k^{(i)}(\mathbf{x}) = \mathbf{x}$.

- If Π_k is a truly random permutation, and if $\mathbf{x}$ is an arbitrary element, what is (a good approximation of) the expected length of the cycle containing $\mathbf{x}$?

Now, let Π be a *pseudo-random* **permutation** family.

- Explain why it must be difficult to discover any input $\mathbf{x}$ that is part of a polynomial size cycle, using only oracle access to Π_k. (poly-size cycle = length of the cycle containing $\mathbf{x}$ is $\leq n^c$ for some constant c>0.)

Question 3. Encryption vs Pseudo-Randomness (2+5+3+5 = 15 points)

Let **Π = (Enc, Dec, Gen)** be a CPA-secure Encryption Scheme. Prove or disprove the following two statements:

a) **Enc** must be a pseudo-random function.

b) **Dec** must be a pseudo-random function.

Let **Π = (Enc, Dec, Gen)** be a CCA-secure Encryption Scheme. Prove or disprove the following two statements:

c) **Enc** must be a pseudo-random function.

d) **Dec** must be a pseudo-random function.

Question 4. Double-AES (15 points)

Consider two possibilities: using AES-256 or using twice AES-128 with independent keys.

Compare those two schemes in as many ways as possible: key size, block size, efficiency and security.
(take for granted that Key-Scheduling is very cheap compared to the other operations)

Question 5. Hashing (10+10+10 = 30 points)

Let **n**=**p**x**q** be a public RSA modulus such that **p** ≡ **q** ≡ 3 (mod 4). Consider the function

$$\mathbf{SQ}(x) = \min\{ x^2 \underline{\text{mod}}\ \mathbf{n}\ , \mathbf{n}\text{-}x^2\ \underline{\text{mod}}\ \mathbf{n} \}$$

where $0 < x < \mathbf{n}/2$.

a) Show that **SQ** is two-to-one over { 1, …, (**n**-1)/2 }.
Why do we use **p** ≡ **q** ≡ 3 (mod 4)?

b) Show that, as a hash function, **SQ** is collision resistant unless **p** and **q** can be found.

c) For a 1024-bit **n**, explain how we may create from **SQ** a collision resistant hash function **SQ'**: $\{0,1\}^* \rightarrow \{0,1\}^{1024}$ that is collision resistant unless **p** and **q** can be found.