Cryptography – Endterm

Abbreviations

- RO = random oracle
- RPO = random permutation oracle
- OWF = one-way function (family/collection)
- OWP = one-way permutation (family/collection)
- TDP = trapdoor one-way permutation
- PRG = pseudorandom generator
- PRF = pseudorandom function
- PRP = pseudorandom permutation
- TBC = tweakable block cipher
- UOWHF = universal one-way hash function (family/collection)
- CRHF = collision resistant hash function (family/collection)
- ES = (private-key) encryption scheme
- PKES = public-key encryption scheme
- MAC = message authentication code
- DSS = digital signature scheme
- DLP = discrete logarithm problem
- CDH = computational Diffie-Hellman problem
- DDH = decisional Diffie-Hellman problem
- $\oplus$ = bitwise XOR

Exercise 1 **6P**

Draw a directed graph with nodes

(A)	computationally secret ES with $\lvert\mathcal{K}\rvert < \lvert\mathcal{M}\rvert$ exist	(B)	RSA problem is hard w.r.t. $\mathsf{Gen}\mathbb{P}^2$
(C)	$\mathbf{NP} \neq \mathbf{P}$ holds	(D)	PRG of variable stretch exist
(E)	CCA-secure ES exist	(F)	OWP exist
(G)	DDH is hard w.r.t. $\mathsf{Gen}\mathbb{QR}_{\text{safe}}$	(H)	OWF exist
(I)	PRF of key and block length n exist	(J)	CDH is hard w.r.t. $\mathsf{Gen}\mathbb{QR}_{\text{safe}}$
(K)	CRHF with sufficient compression exist	(L)	CCA-secure PKES exist

where a **path** from u to v exists *if and only if* the validity of u implies the validity of v **based on the results presented in the lecture**.

Example: $(G) \to (L)$ because of the Cramer-Shoup PKES.

You may merge several nodes into a single node if the validity of any subsumed node implies the validity of any other subsumed node.

Hint: Your graph should have *at most* 9 nodes.

Answer:

Exercise 2 **2P+1P+2P+3P=8P**

(a) Let F be a PRF of key and block length n.

Construct from F a PRP. State all necessary details!

Explicitly state the key and block length of the constructed PRP.

Answer:

(b) Let P be a PRP of key and block length n.

i) Construct from P a PRG of stretch $l(n) = 3n$.

Answer:

ii) Construct from P a CPA-secure private-key encryption scheme.

Remark: It suffices to define Gen and Enc.

Answer:

(c) Let $(\mathsf{Gen}_E, \mathsf{Enc}, \mathsf{Dec})$ be a CPA-secure ES and $(\mathsf{Gen}_M, \mathsf{Mac}, \mathsf{Vrf})$ a secure MAC.

Construct from these a CCA-secure ES $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$.

Explicitly define all three algorithms!

Answer:

Exercise 3 **3P+1P+2P=6P**

A friend of yours proposes the following scheme "PWDF" (password-derivation function) to derive passwords for websites from a secret key:

- Let F be a PRF of block and key length n.
- Let k be a secret n-bit key uniformly chosen at random ($k \overset{u}{\in} \{0,1\}^n$).
- Let $u \in \{0,1\}^*$ be the url of the webpage (in some binary encoding).
- Compute an n-bit password of the url u as follows:

  Partition u into subsequent n-bit blocks $u^{(1)}, \ldots, u^{(l)}$ (pad the last block with 0 if necessary).

  Set $t^{(0)} = 0^n$.

  Compute $t^{(i)} := F_k(t^{i-1} \oplus u^{(i)})$ for i from 1 to l.

  Output $\mathsf{PWDF}_k(u) := t^{(l)}$ as password.

Your friend claims that PWDF satisfies the following security definition:

Every PPT-algorithm $\mathcal{A}$ has only a negligible probability w.r.t. n to succeed in the following experiment:

1. Choose $k \overset{u}{\in} \{0,1\}^n$.
2. Run $(u, w) \overset{r}{:=} \mathcal{A}^{\mathsf{PWDF}_k}(1^n)$.

   $\mathcal{A}$ has *oracle access* to PWDF_k in order to simulate that a password might get stolen from a webpage.

▷ $\mathcal{A}$ succeeds if both (i) $\mathsf{PWDF}_k(u) = w$ **and** (ii) $\mathcal{A}$ has not queried the oracle PWDF_k for the image of u.

(a) Show that your friend is wrong by forging a password for the url $0^n||0^n$.

Answer:

(b) Your friend's security definition has been used for another cryptographic scheme in the lecture.

State the name of this scheme.

Answer:

(c) Briefly describe how PWDF has to be *extended* so that it satisfies the security definition of your friend.

Answer:

Exercise 4 **2P+2P+3P=7P**

Recall: Let N be a positive integer. The Carmichael function maps N to $\lambda(N) := \min\{k > 0 \mid \forall x \in \mathbb{Z}_N^* : x^k \equiv 1 \pmod{N}\}$. For any $a \in \mathbb{Z}$ let $\exp_{a,N} : \mathbb{Z}_N^* \to \mathbb{Z}_N^* : x \mapsto x^a \bmod N$.

(a) Consider specifically $N = 7 \cdot 11 \cdot 13 = 1001$.

Determine the *least positive* $d \in \mathbb{Z}$ such that $\exp_{d,1001}$ is the inverse of $\exp_{7,1001}$.

Remark: $\mathsf{gcd}(7, \lambda(1001)) = 1$.

Answer:

(b) State one reason why modern RSA-based PKES use randomized padding.

In addition, state the name of one such padding scheme used in practice today.

Answer:

(c) Let h be a hash function with output length 256 (in bits), e.g. SHA-256.

Further assume that N is a suitable RSA modulus with $N \in [2^{1024}, 2^{1025}]$.

Finally, let $e, d \in \mathbb{Z}^*_{\lambda(N)}$ with $e \cdot d \equiv 1 \pmod{\lambda(N)}$.

Briefly describe how to compute and verify digital signatures based on the *full-domain-hash* heuristic when (N, e) should be the public verification key, and (N, d) the private signing key.

Solution:

Exercise 5 **1P+2P+2P+2P=7P**

(a) Is 47 a safe prime?

Answer:

(b) Compute the probability that $x \overset{u}{\in} \mathbb{Z}^*_{47}$ is a generator of $\mathbb{Z}^*_{47}$.

Answer:

(c) Is 7 a generator of $\mathbb{Z}_{47}^*$? Prove that your answer is correct.

Answer:

(d) Give a generator of $\mathbb{QR}_{47}$. What is the order of $\mathbb{QR}_{47}$?

Answer:

Exercise 6 **2P+2P+2P=6P**

(a) Let $\langle \mathbb{G}, \cdot, 1 \rangle$ be a finite cyclic group with generator g.

Denote by $q := |\mathbb{G}|$ the order of $\mathbb{G}$.

Assume $q = d \cdot m$ is a composite and let d be a non-trivial factor of q.

Let $y \in \mathbb{G}$.

Show:

If $k \in \mathbb{N}$ satisfies $g^k = y$ in $\mathbb{G}$, then $(k \bmod d)$ is the unique solution of the following problem:

$$\text{Determine } x \in \mathbb{Z}_d \text{ such that } (g^m)^x = y^m \text{ in } \mathbb{G}.$$

Answer:

(b) Given are the prime 89 and the generator 3 of $\langle \mathbb{Z}_{89}^*, \cdot, 1 \rangle$.

Your task is to determine $k \in \mathbb{Z}$ such that $3^k \equiv 86 \pmod{89}$.

Proceed as follows:

i) Using the preceding exercise, first determine k modulo 11.

Answer:

ii) Someone tells you that $k \equiv 5 \pmod 8$. Determine k.

Answer: