ENGG5383: Applied Cryptography **Fall 2015**

Tutorial 1: Introduction

Tutor: Russell W. F. Lai

1.1 Basic Cryptographic Primitives

1.1.1 Notations

- λ (sometimes n or k): *security parameter* (Think of $\lambda = 100$ for 100-bit of security)
- $p(\lambda) = \mathsf{poly}(\lambda)$: $p(\lambda)$ is a polynomial in λ
- $|\mu(\lambda)| \leq \mathsf{negl}(\lambda)$: $|\mu(\lambda)| \leq \frac{1}{p(\lambda)}$ for all $p(\lambda) = \mathsf{poly}(\lambda)$
- PPT: Probabilistic Polynomial (in λ) Time
- $\{0,1\}^n$: The set of n-bit binary strings
- $\{0,1\}^*$: The set of finite-length binary strings
- $\oplus$: bit-wise XOR

1.1.2 Primitives

Definition 1.1 (One-Way Function / Permutation (OWF/P)) *An efficiently computable function $f : D \to R$ is said to be* one-way *if for any PPT adversary $\mathcal{A}$, it holds that*

$$\Pr_{x \in D}\{f(A(f(x))) = f(x)\} \leq \mathsf{negl}(\lambda)\,.$$

Furthermore, if f is bijection, then f is a one-way permutation.

Definition 1.2 (Trapdoor Permutation (TDP)) *A one-way permutation $f : D \to R$ is said to be a trapdoor permutation if there exists a trapdoor t and a polynomial-time algorithm g such that, for all $x \in D$, given $y = f(x)$, we have $x = g(t, y)$.*

Remark 1.3 *Some definitions require the domain D and the space of function and trapdoor pairs be efficiently sampleable.*

Example 1.4 (A "Not Useful" TDP) *Let $f : D_1 \to R_1$ be a TDP. Let $f' : D_1 \times D_2 \to R_1 \times R_2$ be defined as $f'(x_1, x_2) = (f(x_1), x_2)$. Then f' is also a TDP.*

Proof: *Bijectivity and the existence of trapdoor are trivial. Suppose f' is not one-way. Then there exists a PPT adversary $\mathcal{A}'$ such that*

$$\Pr_{(x_1,x_2) \in D_1 \times D_2}\{f'(A'(f'(x_1, x_2))) = f'(x_1, x_2)\} > \mathsf{negl}(\lambda)\,.$$

Let $\mathcal{A}$ be another PPT adversary which, on input $y_1 = f(x_1)$, samples $y_2 \leftarrow D_2$, and passes (y_1, y_2) to $\mathcal{A}'$. $\mathcal{A}'$ returns (x'_1, x'_2) to $\mathcal{A}$, who in turn returns x'_1. Note that

$$\Pr_{x_1 \in D_1}\{f(A(f(x_1))) = f(x_1)\} > \mathsf{negl}(\lambda)\,,$$

which contradicts the fact that f is one-way. ■

Example 1.5 (Candidate OWF based on The Short Integer Solution (SIS) Problem) *Let n, m, $q \in \mathbb{Z}$ such that $m > n$ and $q = n^c$ for some positive integer c. Let $A \leftarrow \mathbb{Z}_q^{n \times m}$ be a random matrix, and $r \leftarrow \mathbb{Z}_q^n$ be a random vector. Let $f_{A,r} : \{0,1\}^m \to \mathbb{Z}_q^n$ be defined as $f_{A,r}(x) = Ax + r$. Then $f_{A,r}$ is a OWF assuming the hardness of SIS.*

Definition 1.6 (Pseudorandom Generators (PRG)) *An efficiently computable function $g : \{0,1\}^\lambda \to \{0,1\}^{\lambda+k}$ for some positive integer k is said to be a pseudorandom generator if for any PPT adversary $\mathcal{A}$, it holds that*

$$|\Pr_{x \in \{0,1\}^\lambda}\{A(g(x)) = 1\} - \Pr_{y \in \{0,1\}^{\lambda+k}}\{A(y) = 1\}| \le \mathsf{negl}(\lambda)\,.$$

Definition 1.7 (Pseudorandom Functions / Permutations (PRF/P) Family) *Let $\mathcal{F} : \mathcal{K} \times D \to R$ be a family of efficiently computable functions indexed by $k \in \mathcal{K}$. For any PPT adversary $\mathcal{A}$, consider the following PPT experiments:*

Real$_\mathcal{A}$*: Sample $k \leftarrow \mathcal{K}$, and give $\mathcal{A}$ oracle access to $f(k, \cdot) \in \mathcal{F}$. After querying polynomial number of times, $\mathcal{A}$ returns a bit b which is returned by the experiment.*

Ideal$_\mathcal{A}$*: Initiates an empty table T. On query x from $\mathcal{A}$, check if $T[x]$ is set. If not, sample $y \leftarrow R$ and assign $T[x] = y$. Reply $\mathcal{A}$ with $T[x]$. After querying polynomial number of times, $\mathcal{A}$ returns a bit b which is returned by the experiment.*

$\mathcal{F}$ is said to be a pseudorandom functions family if for any PPT adversary $\mathcal{A}$, it holds that

$$|\Pr\{\mathbf{Real}_\mathcal{A} = 1\} - \Pr\{\mathbf{Ideal}_\mathcal{A} = 1\}| \le \mathsf{negl}(\lambda)\,.$$

Furthermore, if all $f \in \mathcal{F}$ are bijective, then $\mathcal{F}$ is a pseudorandom permutations family.

Example 1.8 (Simple SKE from PRF) *Let f be a PRF with key k. To encrypt a message $m \in R$, sample $r \leftarrow D$, and output the ciphertext $c = (r, f(k, r) \oplus m)$. To decrypt a ciphertext $c = (c_1, c_2)$, compute $m = c_2 \oplus f(k, c_1)$.*

1.2 Basic Number Theory

1.2.1 Modular Arithmetic

- Consider $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ and $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
- We say that "a is congruent to b modulo n", or $a \equiv b \pmod{n}$, if $a = nx + b$ for some $x \in \mathbb{Z}$.
- Usual arithmetic rules apply:
  1. $a \equiv a \pmod{n}$

2. if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$
3. if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$
4. if $a \equiv b \pmod{n}$ and $c \equiv d$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$
5. if $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$
6. if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for all positive integer k

- Except:
  - if $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$ where $d = \gcd(c, n)$

1.2.2 Fast Exponentiation Algorithm

How to calculate $a^x \pmod{n}$ for large x, say $5^{110} \pmod{131}$?

1. Expand x in binary representation: $110 = 64 + 32 + 8 + 4 + 2$
2. Complete the following table by repeated squaring:

$$\begin{array}{ll} 5^2 \equiv 25 \pmod{131} & 5^4 \equiv 25^2 \equiv 101 \pmod{131} \\ 5^8 \equiv 101^2 \equiv 114 \pmod{131} & 5^{16} \equiv 114^2 \equiv 27 \pmod{131} \\ 5^{32} \equiv 27^2 \equiv 74 \pmod{131} & 5^{64} \equiv 74^2 \equiv 105 \pmod{131} \end{array}$$

3. $5^{110} = 5^{64+32+8+4+2} = 5^{64} \cdot 5^{32} \cdot 5^8 \cdot 5^4 \cdot 5^2 \equiv 105 \cdot 74 \cdot 114 \cdot 101 \cdot 25 \equiv 60 \pmod{131}$.

1.2.3 Euclidean Algorithm

Notations and Terminologies:

- The greatest common divisor (GCD) d of two integers a and b is the maximum of the integers that divides both a and b, denoted as $d = \gcd(a, b)$.
- The integers a and b are said to be *coprime* if $\gcd(a, b) = 1$.
- $a \mid b$ means "a divides b". $a \nmid b$ means "a does not divide b".

Lemma 1.9 *If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.*

Proof: Let $d = \gcd(a, b)$, then $d \mid a$ and $d \mid b$. Then $d \mid (r = a - qb)$. Suppose c is a common divisor of b and r, then $c \mid (a = qb + r)$. By definition of d, $c \leq d$. Therefore $d = \gcd(b, r)$. ■

Theorem 1.10 *For non-zero integers a and b, there exists integers x and y such that $\gcd(a, b) = ax + by$.*

Proof: We provide a constructive proof, *i.e.* we state the (extended) Euclidean algorithm which computes the GCD, x and y. Without loss of generality, assume $a > b > 0$. Compute the following:

$$\begin{aligned} a &= q_1 b + r_1 && 0 < r_1 \le b \\ b &= q_2 r_1 + r_2 && 0 < r_2 \le r_1 \\ r_1 &= q_3 r_2 + r_3 && 0 < r_3 \le r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n && 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

By Lemma 1.9, $\gcd(a, b) = \gcd(b, r_1) = \ldots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$.

Now, we work backward from the second last equation.

$$\begin{aligned} r_n &= r_{n-2} - q_n r_{n-1} \\ &= (1 + q_n q_{n-1}) r_{n-2} + (-q_n) r_{n-3} \\ &= \ldots \\ &= ax + by \end{aligned}$$

■

Example 1.11 *Compute* $\gcd(360, 924)$.

$$\begin{aligned} 924 &= 2 \times 360 + 204 \\ 360 &= 1 \times 204 + 156 \\ 204 &= 1 \times 156 + 48 \\ 156 &= 3 \times 48 + 12 \\ 48 &= 4 \times 12 + 0 \end{aligned}$$

$$\begin{aligned} \gcd(360, 924) = 12 &= 156 - 3 \times 48 \\ &= 156 - 3 \times (204 - 156) \\ &= 4 \times 156 - 3 \times 204 \\ &= 4 \times (360 - 1 \times 204) - 3 \times 204 \\ &= 4 \times 360 - 7 \times 204 \\ &= 4 \times 360 - 7 \times (924 - 2 \times 360) \\ &= 18 \times 360 - 7 \times 924 \end{aligned}$$

1.2.4 Euler's Phi / Totient Function

Euler's totient function: $\phi(n)$ = "# of positive integers that are less than and coprime with n".

Properties: Let p be prime. Let m, n be positive integers such that $\gcd(m, n) = 1$.

- $\phi(p) = p - 1$
- $\phi(p^k) = p^{k-1}(p - 1)$
- $\phi(mn) = \phi(m)\phi(n)$.
  Proof: Consider the following array:

$$\begin{array}{cccccc} 1 & 2 & \ldots & r & \ldots & m \\ m+1 & m+2 & & m+r & & 2m \\ 2m+1 & 2m+2 & & 2m+r & & 3m \\ \vdots & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & & (n-1)m+r & & nm \end{array}$$

For each row, we know by Lemma 1.9 that $\gcd(km + r, m) = \gcd(r, m)$. Therefore there are exactly $\phi(m)$ columns in each row that are coprime with m. Now consider the r-th column, none of them are congruent to each other modulo n. Therefore they are congruent to $0, 1, \ldots, n-1$ in some order, and exactly $\phi(n)$ of them are coprime with n.

■

1.2.5 Fermat's Little Theorem and Euler's Generalization

Theorem 1.12 *(Fermat's Little Theorem) Let p be a prime and $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Theorem 1.13 *(Euler's Generalization of Fermat's Little Theorem)*

If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof: Let $a_1, a_2, \ldots, a_{\phi(n)}$ be positive integers that are less than and coprime with n. Since $\gcd(a, n) = 1$, $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order. Let $aa_i \equiv a'_i \pmod{n}$ for $i = 1, 2, \ldots, \phi(n)$. Then

$$\begin{aligned}(aa_1)(aa_2)\ldots(aa_{\phi(n)}) &\equiv a'_1 a'_2 \ldots a'_{\phi(n)} \pmod{n} \\ &\equiv a_1 a_2 \ldots a_{\phi(n)} \pmod{n}\end{aligned}$$

and so

$$a^{\phi(n)}(a_1 a_2 \ldots a_{\phi(n)}) \equiv a_1 a_2 \ldots a_{\phi(n)} \pmod{n}$$

Since $\gcd(a_i, n) = 1$ for all i, we have $\gcd(a_1 a_2 \ldots a_{\phi(n)}, n) = 1$. Therefore $a^{\phi(n)} \equiv 1 \pmod{n}$. ■

Definition 1.14 (Orders and Primitive Roots) *Given $a \in \mathbb{Z}$, let $k \leq \phi(n)$ be the smallest positive integer such that $a^k \equiv 1 \pmod{n}$. Then k is called the* order *of a. If a has the highest order, namely $\phi(n)$, then a is called a* primitive root *of n. A primitive root a* generates *all the integers less than and coprime with n by self multiplication.*

Example 1.15 *3 is a primitive root of 7.*

x	1	2	3	4	5	6
$3^x \pmod 7$	3	2	6	4	5	1

1.2.6 Chinese Remainder Theorem (CRT)

Theorem 1.16 (Chinese Remainder Theorem (CRT)) *Let $n_1, \ldots, n_k \in \mathbb{N}$ be pair-wise coprime. Then for any $a_1, \ldots, a_k \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that $x \equiv a_i \pmod{n_i}$ for $1 \leq i \leq k$. Furthermore, all solutions x are congruent modulo the product $N = n_1 \cdot n_k$. Hence, $x \equiv y \pmod{n_i}$ for $1 \leq i \leq k$ if and only if $x \equiv y \pmod{N}$.*

Proof: Let $N = n_1 \cdot n_k$ and $N_i = N/n_i$. Since $\gcd(n_i, n_j) = 1$ for all $i \neq j$, we have $\gcd(N_i, n_i) = 1$. Let x_i be the unique solution for $N_i x_i \equiv 1 \pmod{n_i}$ for each i. Consider $x_0 = \sum_i a_i N_i x_i$. Obviously, $x_0 \equiv a_i \pmod{n_i}$ for all i. For the uniqueness of x_0 modulo N, suppose there is another solution x'_0 such that $x_0 \equiv x'_0 \equiv a_i \pmod{n_i}$ for all i. Thus $n_i \mid (x_0 - x'_0)$ for all i. Hence $(N = \Pi_i n_i) \mid (x_0 - x'_0)$. In other words, $x_0 \equiv x'_0 \pmod{N}$. ■

1.2.7 Quadratic Residues

Definition 1.17 *(Quadratic Residues) An integer a is said to be a quadratic residue modulo n if there exists an integer x such that $a \equiv x^2 \pmod{n}$. Other, a is said to be a quadratic non-residue.*

Lemma 1.18 *Let p be an odd prime, g be a primitive root of p. Then for any element $a \equiv g^z \pmod{p}$, the following statements are equivalent:*

1. *a is a quadratic residue.*
2. *z is even.*
3. *$a^{(p-1)/2} \equiv 1 \pmod{p}$. (Euler's criterion)*

The Legendre symbol of a modulo p is defined as $\left(\frac{a}{p}\right) = a^{(p-1)/2}$. Therefore

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a \text{ is a quadratic residue and } p \nmid a \\ -1 & a \text{ is a quadratic non-residue} \end{cases}$$

Proof: The equivalence of the first two statements is trivial.

For the third statement, suppose a is a quadratic residue modulo p, then there exists an integer x such that $a \equiv x^2 \pmod{p}$. Then $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{1}$ by Fermatt's little theorem.

Conversely, suppose $a^{(p-1)/2} \equiv 1 \pmod{1}$. Let g be a primitive root modulo p. Then $a \equiv g^z \pmod{p}$ for some integer z. We have $a^{(p-1)/2} \equiv g^{z(p-1)/2} \equiv 1 \pmod{1}$. Since g is a primitive root, it has order $p-1$. Thus, $p-1 \mid z(p-1)/2$, which means z is even. Thus, a is a quadratic residue.

■

1.3 Basic Abstract Algebra

Definition 1.19 (Groups) *Let $\mathbb{G}$ be a set and "$\cdot$" be an operation defined over $\mathbb{G}$. $(\mathbb{G}, \cdot)$ or simply $\mathbb{G}$ is called a group if the following holds.*

1. *Closed: If $a, b \in \mathbb{G}$, then $a \cdot b \in \mathbb{G}$*
2. *Associative: If $a, b, c \in \mathbb{G}$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*
3. *Existence of Identity: $\exists\ e \in \mathbb{G}$ such that $a \cdot e = e \cdot a = a\ \forall\ a \in \mathbb{G}$*
4. *Existence of Inverses: If $a \in \mathbb{G}$, then $\exists\ a^{-1} \in \mathbb{G}$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$*

Furthermore, if $\mathbb{G}$ is commutative, i.e. "if $a, b \in \mathbb{G}$, then $a \cdot b = b \cdot a$", then $\mathbb{G}$ is said to be an Abelian group. If the number of elements in $\mathbb{G}$ is finite, $\mathbb{G}$ is said to be a finite group. In this case, the number of elements $|\mathbb{G}|$ is called the order of the group $\mathbb{G}$. Otherwise, $\mathbb{G}$ is said to be an infinite group.

Definition 1.20 (Cyclic Groups and Generators) *Let $\mathbb{G}$ be a finite group with order n and identity element $1_{\mathbb{G}}$. If there exists an element $g \in \mathbb{G}$ such that $\mathbb{G}$ can be written as $\{g, g^2, g^3, \ldots, g^n = 1_{\mathbb{G}}\}$, then $\mathbb{G}$ is said to be a cyclic group, and g is said to be a generator of $\mathbb{G}$.*

Example 1.21 *Let $n \in \mathbb{Z}$. $(\mathbb{Z}_n, +)$ is a cyclic group of order n, and any $g \in \mathbb{Z}_n^*$ is a generator of $\mathbb{Z}_n$. Furthermore, if $n = 2, 4, p^k$ or $2p^k$ for some odd prime p and positive integer k, then $(\mathbb{Z}_n^*, \times)$ is a cyclic group of order $\phi(n)$, and any primitive root of n is also a generator of $\mathbb{Z}_n^*$.*

Definition 1.22 (Rings) *Let $(R, +)$ be an Abelian group and "$\cdot$" be an additional operation defined over R. $(R, +, \cdot)$ or simply R is called a ring if the following holds.*

1. *Associative w.r.t. $\cdot$: If $a, b, c \in R$ then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*
2. *Existence of Identity w.r.t. $\cdot$: $\exists\ e \in R$ such that $a \cdot e = e \cdot a = a\ \forall\ a \in R$*
3. *Distributive w.r.t. $+$: If $a, b, c \in R$ then $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ and $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$*

Furthermore, if R is commutative w.r.t. $\cdot$, i.e. "if $a, b \in R$, then $a \cdot b = b \cdot a$", then R is said to be a commutative ring.

Definition 1.23 (Fields) *A commutative ring $(\mathbb{F}, +, \cdot)$ is called a field if multiplicative inverses exist except for the additive identity.*

1.4 Computationally Hard Problems

Definition 1.24 (Integer Factoring Problem) *Given that $N = pq$ for some randomly chosen λ-bit long primes p and q, find p and q.*

Definition 1.25 (Discrete Logarithm Problem (DLP)) *Let $\mathbb{G}$ be a cyclic group of λ-bit long prime order p. Given $(g, y = g^x, p)$ where $g \in \mathbb{G}$ is a generator, and $1 \leq x \leq p$ is randomly chosen, find x.*

Example 1.26 *Let $\mathbb{G}$ be a cyclic group of prime order p with generator g. Let $f : \mathbb{Z}_p^* \to \mathbb{G}$ be defined as $f(x) = g^x$. Then f is a OWP assuming the hardness of DLP.*

Proof: *One-wayness is trivial by the hardness of DLP. f is bijective since $\mathbb{G}$ is cyclic.* ■

Definition 1.27 (RSA Problem) *Given a tuple (N, e, c), where $N = pq$ for some randomly chosen λ-bit long primes p and q, $e \leftarrow \mathbb{Z}^* \phi(n)$, and $c = m^e \pmod n$ for some $m \leftarrow \mathbb{Z}_n^*$, find m.*

Definition 1.28 (Short Integer Solution (SIS) Problem) *Given a tuple (A, n, m, q, β), where $A \leftarrow \mathbb{Z}_q^{n \times m}$, find $s \in \mathbb{Z}^m$ such that $\|s\| \leq \beta$ and $As = 0$.*