CSc 466/566

Computer Security

11 : Midterm Review

Version: 2012/03/27 13:31:26

Department of Computer Science
University of Arizona

collberg@gmail.com

Christian Collberg

Outline

Modular multiplication

- Create the modular multiplication table for Z_7, $xy \bmod 7$.

Modular addition

- Create the modular addition table for Z_7, $x + y \bmod 7$.

Extended Euclidean Algorithm

- Use the Extended Euclidean Algorithm to compute i and j such that
$$\mathrm{GCD}(65, 40) = 65 \cdot i + 40 \cdot j$$
- Source: http://www.mast.queensu.ca/~math418/m418oh/m418oh04.pdf

Extended Euclidean Algorithm

- Use the Extended Euclidean Algorithm to compute i and j such that

$$\mathrm{GCD}(1239, 735) = 1239 \cdot i + 735 \cdot j$$

- Source: http://www.mast.queensu.ca/~math418/m418oh/m418oh04.pdf

Modular Exponentiation

- Create the modular exponentiation table for Z_7, $x^y \bmod 7$.
- Highlight modular inverses

Totient

1. Define $\phi(n)$.
2. What's $\phi(43)$?
3. What's $\phi(42)$?
4. List the elements of Z_{42}^*

Corollary to Euler's Theorem

1. What are the prime factors of 77?
2. What's $\phi(77)$?
3. Use Euler's theorem to compute 20^{62} mod 77.

Modular Multiplicative Inverses

- Computer the modular multiplicative inverse of 7 mod 11, i.e. find x such that $7 \cdot x \bmod 11 = 1$.

Discrete logs

1. Is 3 a primitive root of 11?
2. Is 2 a primitive root of 11?

Outline

RSA Encryption

- Show the result of encrypting $M = 4$ using the public key $(e, n) = (7, 209)$ in the RSA cryptosystem. Be efficient!

RSA Key generation

1. Generate an RSA key-pair using $p = 23$, $q = 13$, $e = 7$.
2. Hint: $\mathrm{GCD}(7, 264) = 1 = (-113) \times 7 + (3) \times 264$
3. Encrypt $M = 88$.
4. Decrypt the result from 2.
5. http://banach.millersville.edu/~bob/math478/ExtendedEuclideanAlgorithmApplet.html

Homomorphic encryption

1. Show that, for RSA encryption

$$E_k(M_1) \cdot E_k(M_2) = E_k(M_1 \cdot M_2)$$

   i.e., RSA is homomorphic in multiplication.

Elgamal encryption

1. Given the prime $p = 11$, the generator $g = 2$ for Z_{11}, and the random number $x = 9$, compute Bob's private and public Elgamal keys.
2. Encrypt the message $M = 11$ using the random number $k = 7$.
3. Decrypt the ciphertext from 2.

Elgamal encryption...

a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1

Diffie-Hellman Key Exchange

- Let $p = 11$.
- Let $g = 2$.
- Let Alice's secret $x = 7$.
- Let Bob's secret $y = 9$.

1. Compute K_1.
2. Compute K_2.

Outline

Attack tree

- Construct an attack tree for how to get a free lunch at a restaurant!
- Source: http://www.win.tue.nl/~sjouke/publications/papers/attacktrees.pdf .

Outline

Symmetric Ciphers: Confusion and Diffusion

- DES is a combination of two basic principles, confusion and diffusion. How do each transform the plaintext into ciphertext?

Outline

Digital Signatures: Definitions

- Define the following terms:
  1. Nonforgeability
  2. Nonmutability
  3. Nonrepudiation

RSA signature: Nonmutability

- Show how the RSA signature scheme does not achieve nonmutability.
- Is this usually a problem? Why?

Cryptographic Hash Function Collision Resistance

- What is the difference between weak and strong collision resistance?

Merkle-Damgård Construction

- Show how, given a compression function C, a long message M can be hashed using the Merkle-Damgård Construction.

Security of Cryptographic Hash Functions

- Assume our hash function H has b-bit output.
- The number of possible hash values is 2^b.
- Attack:
  1. Eve generates large number of messages $m_1, m_2, \ldots$.
  2. She computes their hash values $H(m_1), H(m_2), \ldots$.
  3. She waits for two messages m_i and m_j such that $H(m_i) = H(m_j)$.
- Eve needs to generate $\approx 2^b$ inputs to find a collision, right or wrong? Why?

Outline

Secure boot vs. Authenticated boot

- What is the difference between Secure boot and Authenticated boot?

TPM

1. What are the basic things you need to trust in a TPM-based system?
2. What are the three main life-time events of a TPM chip?

TPM Challenge

- Describe the events that occur during a TPM challenge!

TPM Sealing

- Describe how the TPM can be used for Digital Rights Management of digital media and software!

SetUID Vulnerability

- Show how a malicious user can abuse a setUID program to gain root access!