Lecture 6: Cryptographic Algorithms

Homeworks:

You are given three single-word passwords encrypted using the ciphers presented in this lecture. To be more secure, some passwords are encrypted using more than one cipher. Your task is to determine which ciphers were used and decrypt the passwords.

Encrypted password1 = CMUIAINOMNCTO
Encrypted password2 = VHFUHW
Encrypted password3 = WGIIVX

What was password1 before encryption?
Answer: COMMUNICATION (transposition cipher)

What was password2 before encryption?
Answer: SECRET (Caesar with rotation 3)

What was password3 before encryption?
Answer: SECRET -> VFHHUW (transposition cipher) -> WGIIVX (Caesar with rotation 1)

RSA and Digital Signature: Let be p = 17 and q = 11. Also, assume that RSA chooses e = 7 and d = 23 as encryption and decryption keys, respectively. Given these values of p, q, e, and d,

a) calculate your public and private keys using RSA.
b) Then, assume you want to exchange your clear text message m = 5 securely. Encrypt m with your public key and decrypt the encrypted text again with your private key.
c) Sign the message m=5 with the private key and verify it with the corresponding public key.

Solution:

1. Compute **n = p * q = 17 * 11 = 187**

2. Compute **φ(n) = (p - 1) * (q - 1) = 16 * 10 = 160**

3. Choose **e = 7** as the encryption key.
   - Note that $1 < e = 7 < \varphi(n) = 160$ and
   - e = 7 and φ(n) = 160 are coprime

4. Compute a value for the decryption key d such that
   - (d * e) % φ(n) = 1.
   - One solution is **d = 23** because (23 * 7) % 160 = 1

5. Public key is **(e, n) => (7, 187)**

6. Private key is **(d, n) => (23, 187)**

Encrypt m = 5 with the public key **(e, n) => (7, 187)**:

7. Compute $c = m^e \% n$ => **$c = 5^7 \% 187 = 146$**

Decrypt c with the private key **(d, n) => (23, 187)**

8. Compute $m = c^d \% n$ => **$m = 146^{23} \% 187 = 5$**

Digital Signature

Sign m = 5 with the private key **(d, n) => (23, 187)**

9. Compute $c = m^e \% n$ => **$c = 5^{23} \% 187 = 180$**

Verify the signature c with the public key **(e, n) => (7, 187)**:

10. Compute $m = c^d \% n$ => **$m = 180^7 \% 187 = 5$**

Diffie Hellman: Let be p = 11 and g = 5. Also, assume that Alice and Bob choose a = 7 and b = 3, respectively. Given these values of p, g, a, and b, calculate the shared session secret for Alice and Bob.

Solution

1. Using the random numbers a and b as well as the two common numbers p and g,
   i. Alice computes **$A = g^a \% p = 5^7 \% 11 = 3$**
   ii. Bob computes **$B = g^b \% p = 5^3 \% 11 = 4$**

1. Alice and Bob exchange the numbers **A = 3** and **B = 4** mutually.

2. Alice and Bob calculate the common key k as follows:

   Alice computes **$k = B^a \% p = 4^7 \% 11 = 5$**

   Bob computes **$k = A^b \% p = 3^3 \% 11 = 5$**

3. Alice and Bob use the key **k = 5** to encrypt and decrypt the data

Hash Functions: In order to calculate the numerical representation of m, we can use the table below, which shows the mapping between letters and their numerical codes. We can just sum up the codes of each character for a given input string to obtain its numerical representation. For example: HELLO = 8 + 5 + 12 + 12 + 15 = 52

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

As shown in the table below, you are given four single-word messages and the corresponding (sent) hash values (p and c values are set to 31 and 0.56, respectively). Some messages were manipulated by an unauthorized user. Your task is to verify the sent hash values of each message to determine which messages are manipulated.

Hash function	**Message**	**Sent Hash Value**	**Calculated Hash Value**	**Message Verified / Manipulated**
Division Hashing	MORNING	28	m=13+15+18+14+9+14+7=90 $h_{div}(90) = 90 \bmod 31 = 28$	Verified

Division Hashing	REGARDS	30	m=18+5+7+1+18+4+19=72 $h_{div}(72) = 72 \bmod 31 = 10$	Manipulated
Multiplicative Hashing	SECURITY	13	m=19+5+3+21+18+9+20+25=120 $h_{mult}(120)$= floor(31 * (120 * 0.56 mod 1)) = 6	Manipulated
Multiplicative Hashing	HASHING	29	m=8+1+19+8+9+14+7=66 h_{mult} (66)= floor(31 * (66 * 0.56 mod 1)) = 29	Verified