Introduction to Cryptography
Assignment 4
Xian Mardiros
Dec. 8, 2022

Question 1

Consider the following variation of the Merkle-Damgard transform:

Let (Gen,h) be a compression function with input messages of length 2n and output of length n. Construct a hash function as follows:

- Gen: Same as in compression function (Gen, h)
- H: on input a key s and a string $x \in \{0,1\}^*$ do the following
  - append a 1 to x, followed by enough zeroes so that the length of the resulting string is a multiple of n. Parse the resulting string as the sequence of n-bit blocks $z_0, x_1, x_2, \ldots, x_B$
  - for $i = 1,2,\ldots,B$ compute $z_i = h^s(z_{i-1}) \| x_i$
  - output z_B as the has value of z

Find a collision in this hash function. That is, find $x \neq x'$ such that $H^s(x) = H^s(x')$

Answer

This hash function is vulnerable because the adversary is able to set z_0 instead of having it set as a randomized IV.

For n, and any message where $|m| \geq n$, a collision can be found when the the second-last output of the hash function, z_{B-1} is used as the input message, concatenated to the last block of the original resulting block sequence, ie. $H^s(z_{B-1}^m \| x_B^m) = H^s(m)$.

Example:

For n=3, the adversary picks value $m_1 = (000 \;\; 000)$. This is turned into the block sequence $z_0^1 \| x_1^1 \| x_2^1 = (000 \;\; 000 \;\; 100)$. This creates the hash results $z_0^1 = 000$, $z_1^1 = h^s(z_0^1 \| x_1^1)$ and $z_2^1 = h^s(z_1^1 \| x_2^1) = z_B^1$. The adversary picks the second message $m_2 = z_1^1$. This is then turned into the block sequence $z_1^1 \| 100 = z_1^1 \| x_2^1 = z_1^1 \| x_2^2$. Note that $x_2^1 = x_2^2$. The hash result is $z_1^2 = h^s(z_1^1 \| x_2^1) = z_B^2$.

Since $z_B^1 = z_B^2$, we have a hash collision.

Question 2

Alice publishes her public key for RSA encryption as follows: modulus n = 133 and (encryption) exponent e = 7

1. Bob wants to send alice the message m=3. What ciphertext does bob send to alice?
2. Compute the decryption exponent d for alice
3. Suppose alice receives the ciphertext c=2 from bob. What is the plaintext?

1: encrypt m=3

n = pq = 133, e=7

ciphertext is c = m^e = 3^7 (mod 133) = 3^5*3^2(mod 133) = 243*3^2(mod 133) = 110 *3^2(mod 133) = 330 * 3 (mod 133) = 64*3 (mod 133) = 59

2: compute decryption exponent

decryption exponent d is the inverse of e.

to compute d, first need phi(n) = (q-1)(q-1). The prime factors of 133 are 7 and 19, and so $\phi(n)=(q-1)(p-1)=6\cdot 18=108$. It is acceptable to assume that the prime factors are known, since in reality, n would have been calculated from them, and not the other way around. Using extended Euclidean algorithm, find $d=7^{-1}(mod\,108)$

Euclidian algorithm:
$108=15\cdot 7+3$
$7=2\cdot 3+1$
$3=2\cdot 1+1$
$1=1\cdot 1+0$

j	0	1	2	3	4
qi	-	15	2	2	1
ti	0	1	-15	31	-77

So (-77)(7) = (31)(7) = 1 (mod 108). So d = 31

3. Compute plaintext from ciphertext c = 2

m = c^d (mod n) = 2^{31} (mod 133) = 79

Question 3

in RSA, the modulus value n = pq is public but $\phi(n)$ is private. Show how an adversary could determine p and q if they had $\phi(n)$.

The value of n is public, so

$(p-1)(q-1)=\phi(n)$ and $pq=n$

Find values p and q such that $\phi(n)=(p-1)(q-1)=pq-q-p+1=n-q-p+1$.

Combining this with $pq=n$, we can obtain the quadratics:

$$\phi(n)=n-\frac{n}{p}-p+1\Rightarrow 0=-p^2+p(n+1-\phi)-n \quad \text{and} \quad 0=-q^2+q(n+1-\phi)-n$$

The two quadratics are the same, and applying the quadratic formula will give two solutions, which are the values of p and q.

For example, for the previous question $\phi(n)=108, n=133$. Applying the quadratic formula to the roots of the polynomial $y=-x^2+x(133+1-108)-133=-x^2+x(26)-133$ gives the solutions x=7,19, which are the primes given in question 2.

Quadratic formula calculations omitted because this isn’t high school.

Question 4.

For the ElGamal digital signature scheme, suppose prime p = 6961, generator g = 437, signing exponent s = 6104

What is the value of *v*?

Assuming that v is equivalent to β in the lecture notes, then
$v = g^s (mod\ p) = 437^{6104} (mod\ 6961)$

Using the efficient exponentiation algorithm:

The exponent 6104 can be written as $(1011111011000)_2$

The exponentiation calculation was done on libreoffice calc:

I	ki	Z (mod 6961)
		1
12	1	437
11	0	3022
10	1	1066
9	1	3754
8	1	4948
7	1	2985
6	1	716
5	0	4503
4	1	6217
3	1	482
2	0	2611
1	0	2502
0	0	2065

So the final value of *v* is 2065.

What is the signature (S1,S2) for the message m = 5584 when the secret random value for e is e = 4451.

$$Enc_K(x,k) = (y_1, y_2) = (g^k (mod\ p), x\beta^k (mod\ p))$$

Using the notation used in this assignment,
$$(S_1, S_2) = (g^e (mod\ p), m\, v^e) = (437^{4451} (mod\ p), 5584 \times 2065^{4451} (mod\ p))$$

Extending the formulas in libreoffice allows this to be easily calculated. The binary representation of exponent 4451 is 1000101100011.

Calculating S1, which has base 437:

I	ki	Z (mod 6961)
		1
12	1	437
11	0	3022
10	0	6613
9	0	2767
8	1	604
7	0	2844
6	1	1940
5	1	3808
4	0	1101
3	0	987
2	0	6590
1	1	6077
0	1	3534

Calculating S2 which has base 2065:

I	ki	Z (mod 6961)
		1
12	1	2065
11	0	4093
10	0	4483
9	0	882
8	1	2207
7	0	5110
6	1	353
5	1	4220
4	0	2162
3	0	3413
2	0	2816
1	1	5747
0	1	4735
	5584	2362

And so the signature is (3534, 2362)

Question 5.

Show that there exists a message m such that an adversary can forge a signature (S1,S2) using only public information if it also knows that s=e.

Want to find a message from which the values $S_1 = g^s (mod\ p)$ and $S_2 = m\, v^s (mod\ p)$ can be calculated without directly knowing p. Since we know that s=e, and v is calculated using s, we should use v in our calculations somehow.

Forging S1 is trivial, since $S_1 = g^e (mod\ p) = g^e (mod\ p) = v$ which is part of the public key.

For any message m, forging $S_2 = m\, v^s (mod\ p)$ is not trivial, however for the message m=0, the equation becomes $S_2 = 0\, v^s (mod\ p) = 0$.

Therefore, for m=0, the signature can be forged as $(S_1, S_2) = (v, 0)$.

Question 6.

Show that alice and bob output the same key.

$$w \oplus t = (u \oplus r) \oplus t = (s \oplus t) \oplus r \oplus t = (k \oplus r) \oplus t \oplus r \oplus t = k$$

What messages are public?
The messages s, u and w are public.

Since $s = k \oplus r$, $k = s \oplus r$

Since $w = u \oplus r$, $r = w \oplus u$

Therefore $k = s \oplus w \oplus u$