The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security
Week 10 Workshop – 10th and 12th May 2021

Solutions

1. In 1985, T. ElGamal announced a public-key scheme based on discrete logarithms, closely related to the Diffie-Hellman key exchange technique introduced in 1976.
The global elements of ElGamal scheme are a q and α, where q is prime, and α is a primitive root of q. A user A selects a private key X_A and calculates a public key $Y_A = \alpha^{X_A} \bmod q$.

User A encrypts a plaintext $M < q$ intended for user B as follows.
1. Choose a random integer k such that $1 \le k \le q-1$.
2. Compute $K = (Y_B)^k \bmod q$.
3. Encrypt M as the pair of integers (C_1, C_2) where $C_1 = \alpha^k \bmod q$ and $C_2 = K \cdot M \bmod q$.

User B receives the ciphertext (C_1, C_2) and recovers the plaintext as follows:
1. Compute $K = (C_1)^{X_B} \bmod q$. (i.e. use C_1 to recover K)
2. Compute $M = (C_2 \cdot K^{-1}) \bmod q$. (i.e. use K and C_2 to recover M)

Show that the system works (i.e. show that the decryption process recovers the plaintext).

Solution:

We only need to show that $K = (C_1)^{X_B} \bmod q$ and $M = (C2 \cdot K^{-1}) \bmod q$.

$K = (C_1)^{X_B} \bmod q$
$= (\alpha^k \bmod q)^{X_B} \bmod q$
$= \alpha^{kX_B} \bmod q$
$= Y_B^k \bmod q$
$= K$

$M = (C_2 \cdot K^{-1}) \bmod q$
$= (K \cdot M \bmod q) \cdot K^{-1} \bmod q$
$= K \cdot K^{-1} M \bmod q$
$= M$

2. In the RSA public-key encryption scheme, each user has a public key e and a private key d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?

Solution:
No, it is not safe.

If we know d, then we also know (e·d)-1 which is a multiple of $\phi(n)$, as (e·d)mod$\phi(n)=1$. There is a probabilistic algorithm (Las Vegas) that runs in expected polynomial time and yields the factorization $n = p \cdot q$ if $\phi(n)$ is known.

Note that if x^2 mod $n = 1$ then x^2 mod $p = 1$ and x^2 mod $q = 1$.
This is the case if and only if x mod $p = \pm 1$ and x mod $q = \pm 1$.
Solutions x mod $p = x$ mod $q = x$ mod $n = \pm 1$ are trivial.
If we could find one of the other two solutions

x mod $p = 1$, x mod $q = -1$ or
x mod $p = -1$, x mod $q = 1$

(note that here x mod $n \neq \pm 1$)

Then we would have

gcd($x+1$,n) = p or q and
gcd($x-1$,n) = q or p

and it would be straightforward to find p and q (Euclid's algorithm for gcd).

The following is a probabilistic algorithm for finding x.
We pick a random number w such that $1 < w < n$. If gcd(w,n) > 1, we have either p or q. If gcd(w,n) =1 then

w^{ed-1} mod $n = w^{k\phi(n)}$ mod $n = 1$

We can write (ed -1) mod n as $2^s r$ where r is odd. Then we have

$w^{2\wedge s\, r}$ mod $n = 1$

We now need to find t, 0 < t ≤ s, such that $v^2 = w^{2\wedge t\, r}$ mod $n = 1$ and $v \neq \pm 1$.
We can use brute force to find t.

If there is no such t, we need to randomly generate a new w and start all over again. The probability that there will be such t for any given w is > ¾.
Thus on average we will need to generate < 4/3 random numbers w.

3. In an RSA system, the public key of one user is (31, 3599). What is the user's private key?

Solution:
n = 59 × 61
ϕ(n) = 58×60 = 3480
e×d mod ϕ(n) = 1
31×d mod 3480 = 1
3480 = 2^3×3×5×29, thus ϕ(3480) = 2^2×2×4×28 = 896
sing Euler's theorem we get

$d = 31^{895} \bmod 3480 = 31\times31^{894} \bmod 3480 = 31\times (31\times31)^{447} \bmod 3480 =$
$= 31\times961\times (961\times961)^{223} \bmod 3480$
$= 1951\times1321\times (1321\times1321)^{111} \bmod 3480$
$= 2071\times1561\times (1561\times1561)^{55} \bmod 3480 =$
$= 3391\times721\times (721\times721)^{27} \bmod 3480 =$
$= 1951\times1321\times (1321\times1321)^{13} \bmod 3480 =$
$= 2071\times1561\times (1561\times1561)^{6} \bmod 3480 =$
$= 3391\times (721\times721)^{3} \bmod 3480 =$
$= 3391\times1321\times1321^{2} \bmod 3480 =$
$= 751\times1561 \bmod 3480 =$
$= 3031 \bmod 3480 =$
$= 3031$

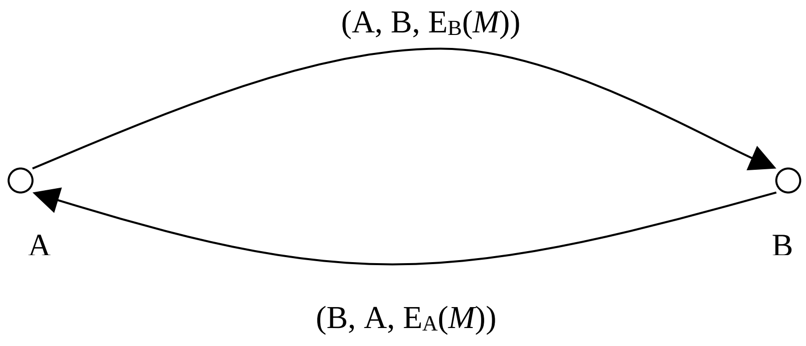
Checking:
$31\times3031 \bmod 3480 = 93961 \bmod 3480 = 1$

4. Prove that RSA public system works correctly even when $\gcd(M, n) \neq 1$.

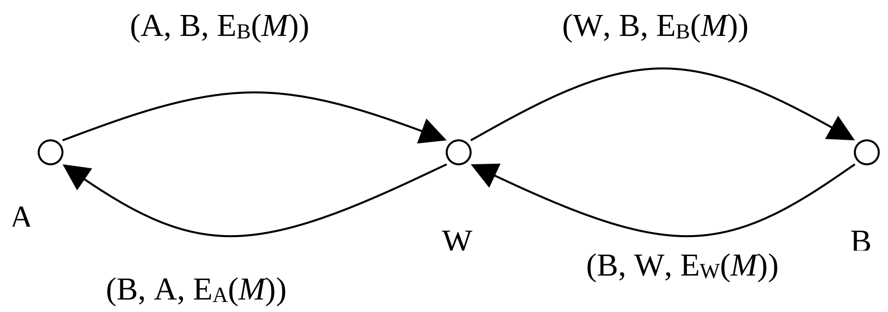
Solution idea:
If $\gcd(M, n) \neq 1$, then M is either a multiple of p or a multiple of q. Prove $M^{k\phi(n)+1} \bmod p = M \bmod p$ separately for $\gcd(M,p) = 1$ and $\gcd(M, p) \neq 1$. Do the same for mod q, and from these two show that $M^{k\Phi(n)+1} \bmod n = M \bmod n$ for all n.

5. Show how an active wiretapper could break the following scheme to determine *M*. Users Alice and Bob exchange a message *M* using the following public-system protocol:

a. Alice encrypts *M* using Bob's public key and sends the encrypted message $E_B(M)$ together plaintext stating both Alice's and Bob's identity, i.e., $(A, B, E_B(M))$
b. Bob deciphers the ciphertext and replies to Alice with $(B, A, E_A(M))$.



Solution:
An active wiretapper Will can intercept the message $(A, B, E_B(M))$ and replace it with $(W, B, E_B(M))$; Bob will reply with $(B, W, E_W(M))$, and Will can find *M* by decrypting $E_W(M)$.



6. Suppose users Alice and Bob exchange a message *M* in a conventional system using a trusted third party S and the protocol given below. Show how an active wiretapper could break the scheme to determine *M* by replaying $E_A(R)$.

c. Alice generates a random number R and sends to S her identity A, destination B and $E_A(R)$.
d. S responds by sending $E_B(R)$ to Alice.
e. Alice sends ($E_R(M)$, $E_B(R)$) to Bob.
f. Bob decrypts $E_B(R)$ and uses *R* to decrypt $E_R(M)$ and get *M*.

Solution:

An active wiretapper Will can pretend to be A, and send [A, W and $E_A(R)$] to S - S will respond with $E_W(R)$. Will can then decrypt $E_W(R)$ and use R to decrypt $E_R(M)$ and get *M*.