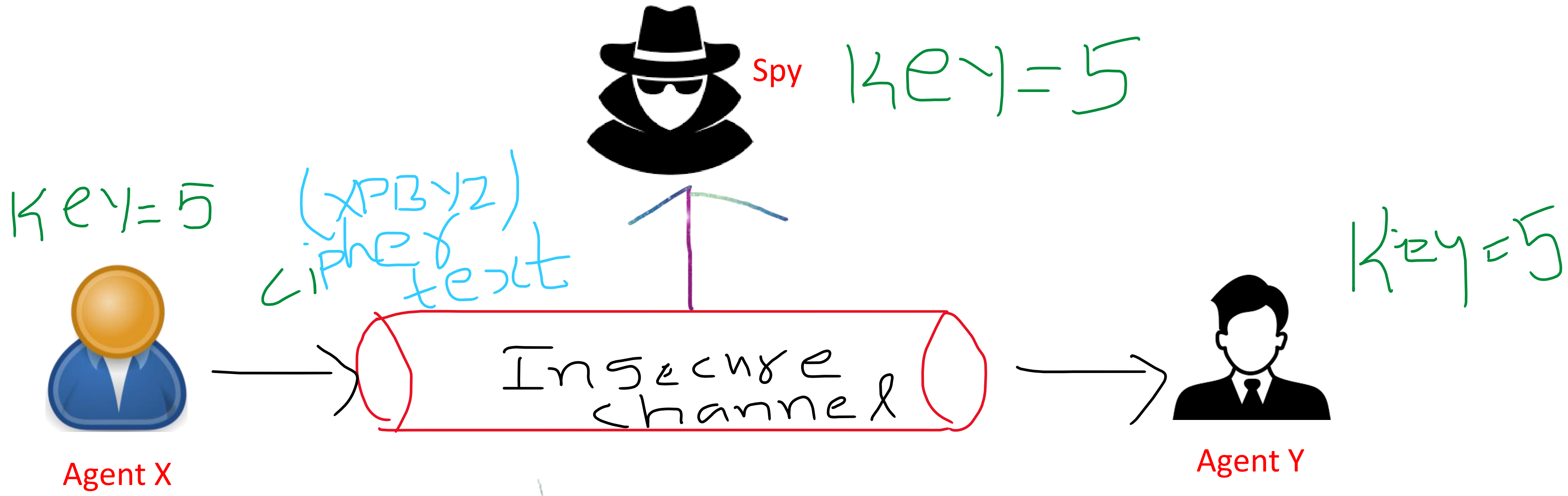
Diffie-Hellman Key Exchange

Module III

Discrete logarithm problem

- $i = dlog_{b,m}(a)$
- a $= b^i (mod\ m)$
- we should get a unique value for i, if b is a primitive root of prime modulo m.
- $? = dlog_{17,2111}(1992)$
- $1922 = 17^i\ (mod\ 2111)$
- Answer: 12

Symmetric key encryption: Big problem



key xchange prbm?

Key Exchange Algorithm

Spy

Select Xa < p
Xa=3.

Xa=3.
$A=g^{Xa} mod\ p$
$A=2^3 mod\ 13$
A=8

$[P=13, g=2]$

p is prime number, g is generator.
g is the primitive root of p

Select Ya < p
Ya=7.

Ya=7.
$B=g^{Ya} mod\ p$
$B=2^7 mod\ 13$
B=11

A=8

B=11

Agent X

Agent Y

$S=B^{Xa} mod\ p$
$S=11^3 mod\ 13$
$\boxed{S=5}$

secret key

$S=A^{Ya} mod\ p$
$S=8^7 mod\ 13$
$\boxed{S=5}$

secret key

public area

Key Exchange Algorithm

Spy

Can the hacker able to compute secret key by knowing p, g, A and B values. ?

Select Xa < p
Xa=3.

Xa=3.
A=$g^{Xa} mod\ p$
A=$2^{3} mod\ 13$
A=8

$[P=13, g=2]$

p is prime number, g is generator.
g is the primitive root of p

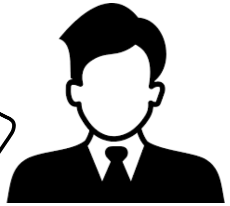
Select Ya < p
Ya=7.

Ya=7.
B=$g^{Ya} mod\ p$
B=$2^{7} mod\ 13$
B=11

A=8

B=11

Agent X



Agent Y

S=$B^{Xa} mod\ p$
S=$11^{3} mod\ 13$
$\boxed{S=5}$

secret key

S=$A^{Ya} mod\ p$
S=$8^{7} mod\ 13$
$\boxed{S=5}$

secret key

public area

Diffie-Hellman Key Exchange

- Published in 1976 by Diffie and Hellman.
- It allows two parties who have not previously met to securely establish a key which they can use to secure their communications.
- The Diffie-Hellman key exchange was the first widely used method of safely developing and exchanging over an insecure channel.
- These keys can then be used with symmetric key algorithms to transmit Information in a protected manner.

Steps in Diffie-Hellman Key Exchange

- Agent X and Agent Y, using insecure communication, agree on a huge prime p and a generator g.
- They don’t care if someone listens in.
- Agent X choses some large random integer Xa < p and keeps it secret.
- Likewise, Agent Y chooses Ya<p and keeps it secret.
- These are their private keys.
- Agent X computes his “public key” $A = g^{Xa} mod\ p$ and sends it to Agent Y using insecure communication.
- Agent Y computes its “public key” $B = g^{Ya} mod\ p$ and sends it to Agent X. Here, 0 < A < p, 0 < B < p.
- Agent X computes S1= $B^{Xa} mod\ p$ and Agent Y computes S2= $A^{Ya} mod\ p$.