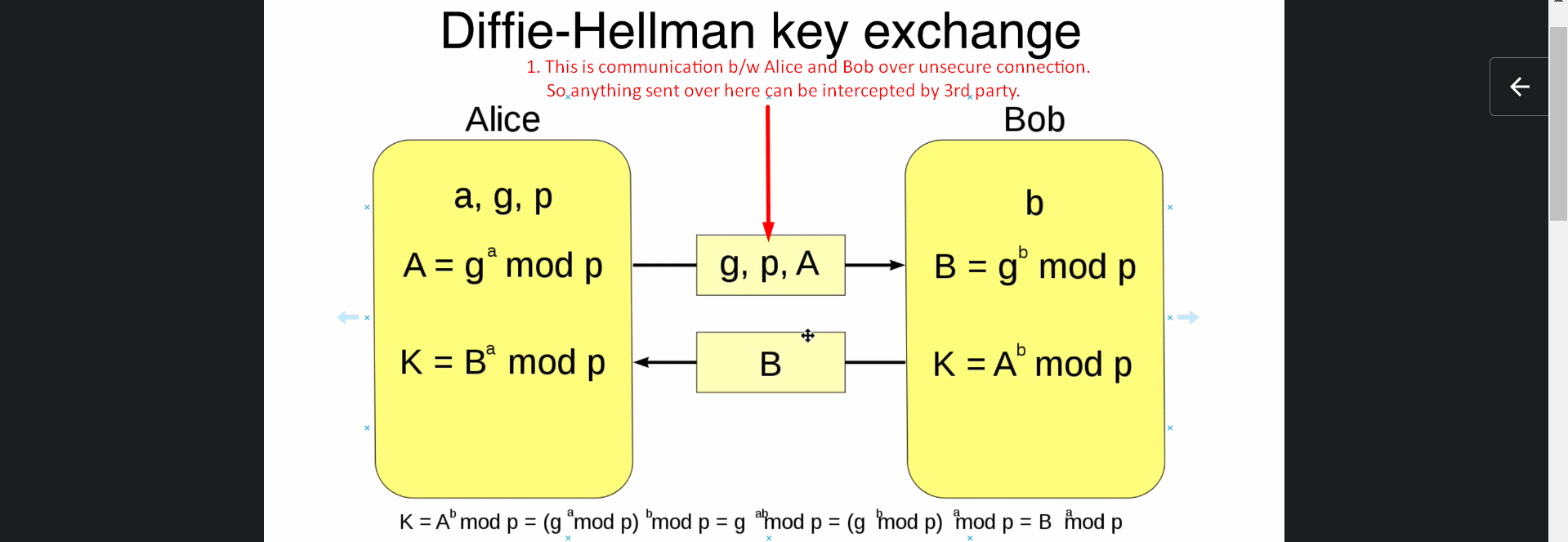
1. As we discussed in last lecture that Modulus is one-way function.
2. Agenda:
   1. Discuss how Diffie Hellman uses Modulus function to generate same key both sides.
3. 
4. As a result of this exchange (g,p,a, B in above slide) and some operations including modulus operation, we will be able to generate same key both sides.
5. Above K is the large key that will be generated both sides.
6. Both sides generate two pairs of public and private key and they need to exchange the public keys with each other.
   1. But to reduce the network packets, Alice generate private number a and two public keys (g, p) and share g, p with Bob along with A.
7. As we can see in the above snapshot, Alice generate 3 numbers **a**, g, p and Bob generates one number **b** where a and b are private keys whereas g and p will be transferred over network and considered to be public keys.
8. Jatin: This is a simple school stuff. Just see what is being assumed and what is being exchanged and how those calculation is being done.   
   At the bottom, there is a proof.
9. Let’s discuss how no one can get same key except Alice and Bob.