Firstly let me tell you about what my company doing. My company is printing company. Regular customer of my company is coming from banking industry and insurance industry. So they buy poster, brochure and business card from my company. To create those product, they use our web application systems to upload required data to us so that we can generate poster or brochure using their data. As they are from financial industry, they need very strong security for those data they gave to us. That is the reason why I involved in the security area.

So, firstly, let me tell you about how I manage security for customer data file. Some customer upload excel data file and some customer upload zip file, but whatever it is, those files are password protected. So our system have to protect user’s data file password. If our system keep password as plain text, then any hacker can get it easily. So I have to encrypt to convert to ciphertext.

So I want to tell a little about how encryption work based on my experience. To make it encrypt my system need to generate secret key so that it can be used to decrypt or to read the ciphertext. It is very simple way for encryption. But It has the problem. Let’s say that user key in the same password for several times, then cipher text will always be the same which is not good. It can make it easy to guess what will be the password. Best practices is to make it harder to guess. So I used IV – Initialization vector which is nothing but a group of random numbers. IV can generate different ciphertext even if user key in the same password for multiple time which make it difficult to guess. It is good practices.