- Eve can decrypt ciphertext C by using her private key.
- Eve now alters the message M into F as F = "My Account Number 98765" and sends F to Bob. She had encrypted F with Y, Bob'public key.
- Bob can decrypt it using his private key and can retrieve F . Now Bob can find that Eve has altered the message using a public-key certificate, Both Alice and Bob can find if Eve is in the middle.

Using a public-key certificate, Both Alice and Bob can find if Eve is in the middle.

4 Why Cryptosystems Fail

4.1 Security of computer systems and it's Evolution

Security had major evolution after world war 2. Before World war 2, security(cryptography) was handled by the government bureaucrats. They were reluctant to accept their failures and hence incidents such as the British Navy codes were cracked by the German. So after the 2nd world war, cryptography was taken over by cryptosystem engineers.

4.2 Building and Operating Secure Systems

The paper clearly states that Implementing secure computer systems using the available encryption products is beyond most organization's' capabilities currently.The flaw in building a secure system happens in many places such as it might the vendor's mistake or the equipment designers mistake or even at the application level.It also suggests 2 methods to tackle such problems, one is to have a certification for the human work involved and the other is a system level approach to designing and evaluating security.The paper also states that the vendor's to train the people who work at the application level to manage the system. It also doesnt want security products to be certified under ITSEC unless the manufacturer can show that both the system factors and the human factors have been properly considered.

4.3 Main proposal of the paper

The main proposal of the paper is to site the various failure models of banking systems.It turns out that the threat model commonly used by cryptosystem designers was wrong: most frauds were not caused by cryptanalysis or other technical attacks, but by implementation errors and management failures. The paper also suggests a new paradigm shifts in cryptography.

4.4 Security in Banking-then and now

There has been a huge amount of change in terms of security in banking sectors then and now. The ATM frauds that were given as examples are reduced to a minimum now as the general public are aware about the Skimmer machines and fraudulent keypads. Moreover all transactions are immediately notified to us by either our email or through our SMS. Regarding the other protection mechanisms, even when we transfer money online we are sent a one time message to our registered account to check as an additional security. Such has been the importance given to security in banking sector now a days.

4.5 Security in other industries to Banking sectors

Security in banking sectors is much more important compared to other industries. Incidents of a single man who looted almost a million dollars from a bank in USA from a home system has been reported.The consequences are much more when a security failure happens in a banking sector and it affects many lives wheras when a security failure happens in a social media only a few persons are affected. Considering this, Security is important in all industries but it is more important when banks are involved.

5 References

https://searchsecurity.techtarget.com/definition/digital-signature
https://en.wikipedia.org/wiki/Collision_resistance
https://simple.wikipedia.org/wiki/Cryptographic_hash_function
https://security.stackexchange.com/questions/12066/can-i-detect-a-mitm-attack—
https://www.protectimus.com/blog/mitm-prevention-and-detection
https://searchsecurity.techtarget.com/definition/public-key-certificate