ARI Interview question

1. Fundamental

* Hãy trình bày tất cả những hướng tiếp cận và cách giải quyết tốt nhất khi bạn được giao hiện thực một chức năng xác thực OTP

Trả lời :

* Theo như em tìm hiểu thì OTP (One Time Password) là 1 đoạn mật khẩu dùng 1 lần, hoặc ngắn hạn, thường dùng để xác thực giao dịch hoặc vấn đề sau cùng. Bản thân em cũng đã từng dùng qua OTP như là giao dịch ngân hàng, đặt lại mật khẩu tài khoản mạng xã hội,vv…
* Theo em cảm nhận thì OTP tuy là bước xác thực cuối cùng nhưng lại là bước rất quan trọng, thực tế thì có rất nhiều chuyện người dùng bị mất tiền trong thẻ ngân hàng chỉ vì cung cấp đoạn mã OTP cho người lạ
* Bằng những kiến thức em tìm hiểu và trải nghiệm được, thì theo em những hướng tiếp cận và cách giải quyết tốt nhất khi hiện thực một chức năng xác thực OTP là :

+ Đầu tiền cần tạo ra được 1 đoạn OTP mà khó có thể đoán được, Vd như 1 đoạn mã gồm 6 chữ số hoặc hơn, hoặc là vừa chữ vừa số, vv… Nên tránh các đoạn mã bảo mật kém, để đoán được, VD như là : 1234,8765,vv… Việc tạo ra đoạn mã này sẽ tuỳ vào ngôn ngữ là người lập trình soạn

+ Sau khi đã có đoạn mã, việc tiếp theo là cần nơi để chứa đoạn mã xác thực này. Em nghĩ trong cơ sở dữ liệu của đối tượng này nên tạo thêm 2 cột, 1 cột để lưu giá trị của mã OTP vừa tạo, 1 cột để lưu thời gian mã OTP hết hạn (Do mã OTP thường có thời hạn ngắn).

+ Sau khi đã có đủ 2 điều kiện trên, thì luồng hoạt động của 1 vòng đời OTP sẽ là :

1. Người dùng gửi 1 hoặc nhiều thông tin để xác thực tài khoản (Số thẻ Ngân Hàng, CMND, SDT, vv…).
2. Hệ thống nhận thông tin trên, tiến hành tra cứu và nếu lọc ra đước tài khoản khớp với thông tin trên, hệ thống sẽ tạo ra 1 đoạn mã OTP ngẫu nhiên. Đoạn mã OTP này và thời hạn sử dụng của nó cũng sẽ được lưu vào cơ sở dữ liệu của tài khoản đó, đồng thời mã OTP này củng sẽ được hệ thống gửi về SDT, hoặc Mail mà người dùng đã dủng để đăng ký tài khoản giao dịch.
3. Tiếp theo sau khi người dùng nhận được đoạn mã OTP, người dùng sẽ gửi lại đoạn mã OTP này về hệ thống. Nếu mã OTP người dùng nhập vào đúng và còn trong thời hạn sử dụng, thì giao dịch đó được xác minh thành công.

* Đó là các hướng tiếp cận và cách giải quyết tốt nhất khi được giao hiện thực một chức năng xác thực OTP mà em nghĩ ra. Nếu có sai sót thì mong các anh có thể chỉ giao lại ạ