The seeds of modern cryptography

1. **Diffusion**
   Mix-up symbols
   Transposition Cipher

2. **Confusion**
   Replace a symbol with another
   Polyaphabetic Cipher

3. **Randomization**
   Repeated encryption of the same text are different
   OTP

A brief history

~ 2000 years ago	Substitution ciphers (a.k.a mono alphabetic ciphers)
Few Centuries Later	Transposition Ciphers
Renaissance	Polyalphabetic Ciphers
1844	Invention of the Telegraph
1882	One Time Pad
1939	World War II The Enigma Machine
1970	Data Encryption Standard (DES)
1976	Public Key Cryptography (RSA)