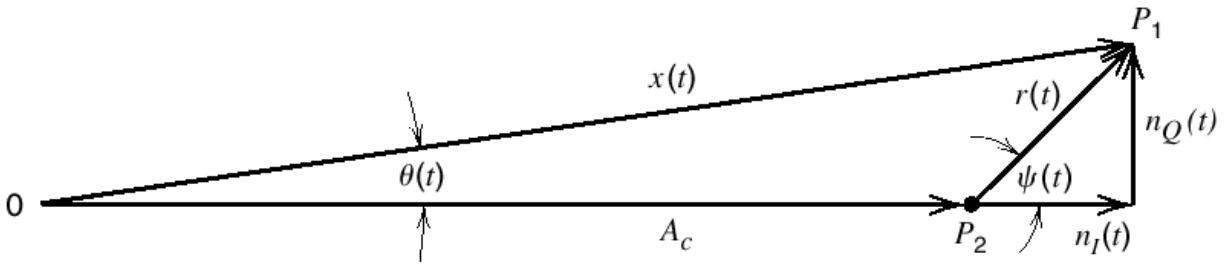
FM Threshold Effect



The composite signal at the frequency discriminator input

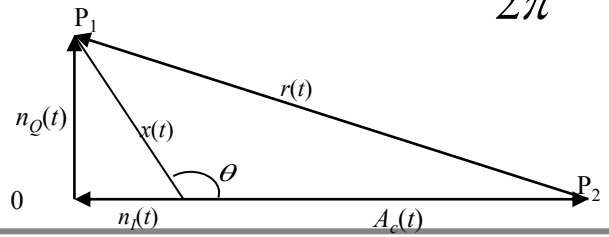
$$x(t) = \left[A_c + n_I(t)\right]\cos(2\pi f_c t) - n_Q(t)\sin(2\pi f_c t) \quad (2.1$$

$$\theta(t) = \tan^{-1}\frac{n_Q(t)}{A_c + n_I(t)}$$

Occasionally, P_1 may sweep around the origin ,

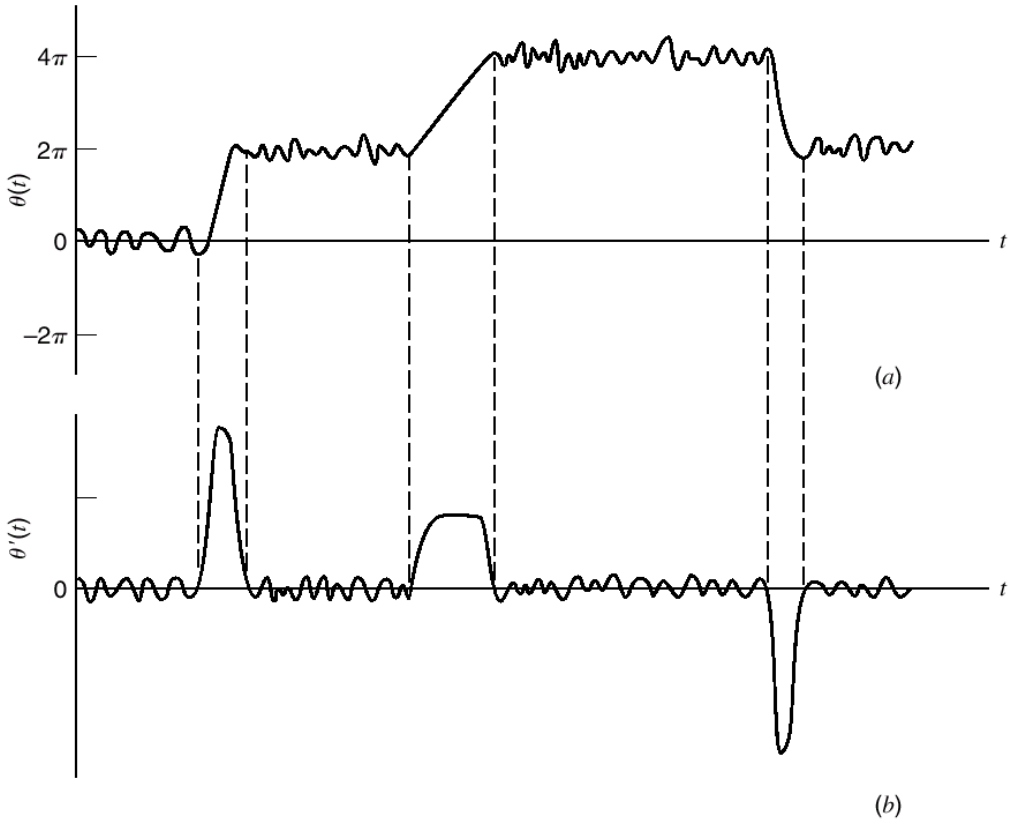
$\theta(t)$ increases or decreases 2π

The discriminator output is equal to $\dfrac{\theta'(t)}{2\pi}$



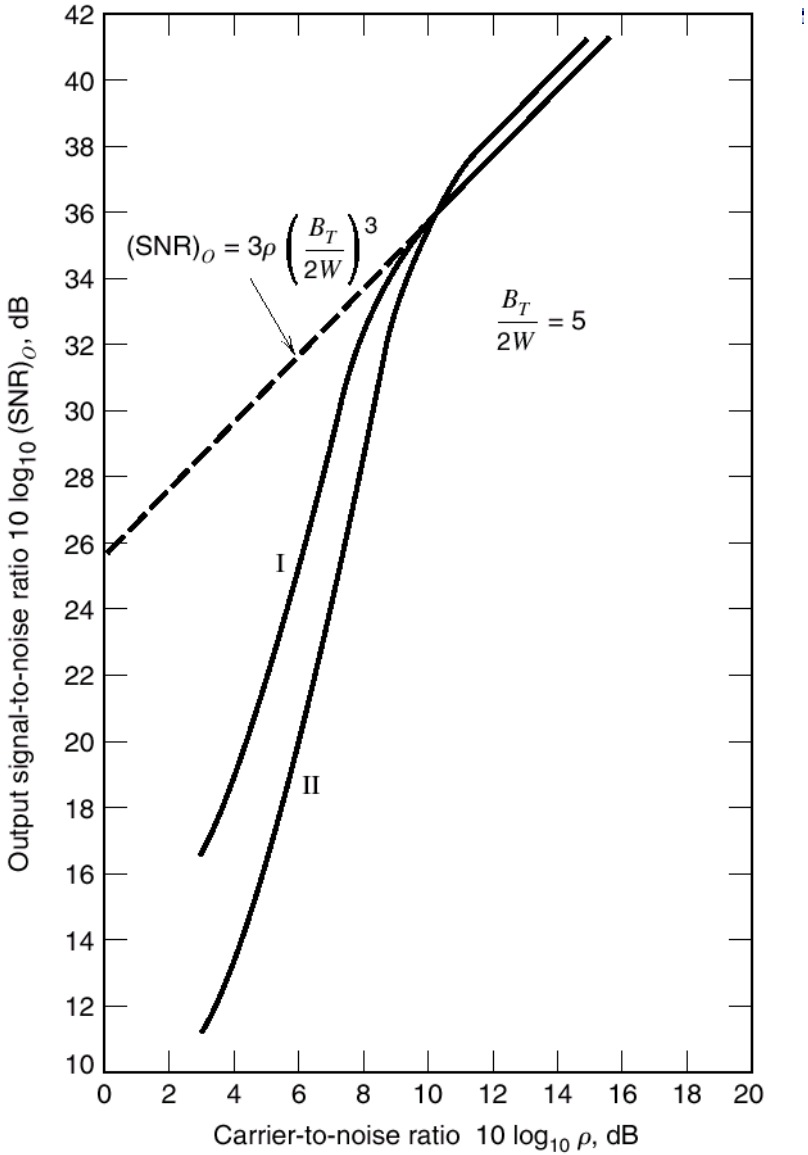
Example

- **I**llustrating impulse ike components in $\theta'(t) = d\theta(t)/dt$ produced by changes of 2π in $\theta(t)$; (a) and (b) are graphs of $\theta(t)$ and $\theta'(t)$, respectively.



Threshold Effect

- Dependence of output signal-to-noise ratio on input carrier-to-noise ratio for FM receiver. In curve I, the average output noise power is calculated assuming an unmodulated carrier. In curve II, the average output noise power is calculated assuming a sinusoidally modulated carrier. Both curves I and II are calculated from theory.

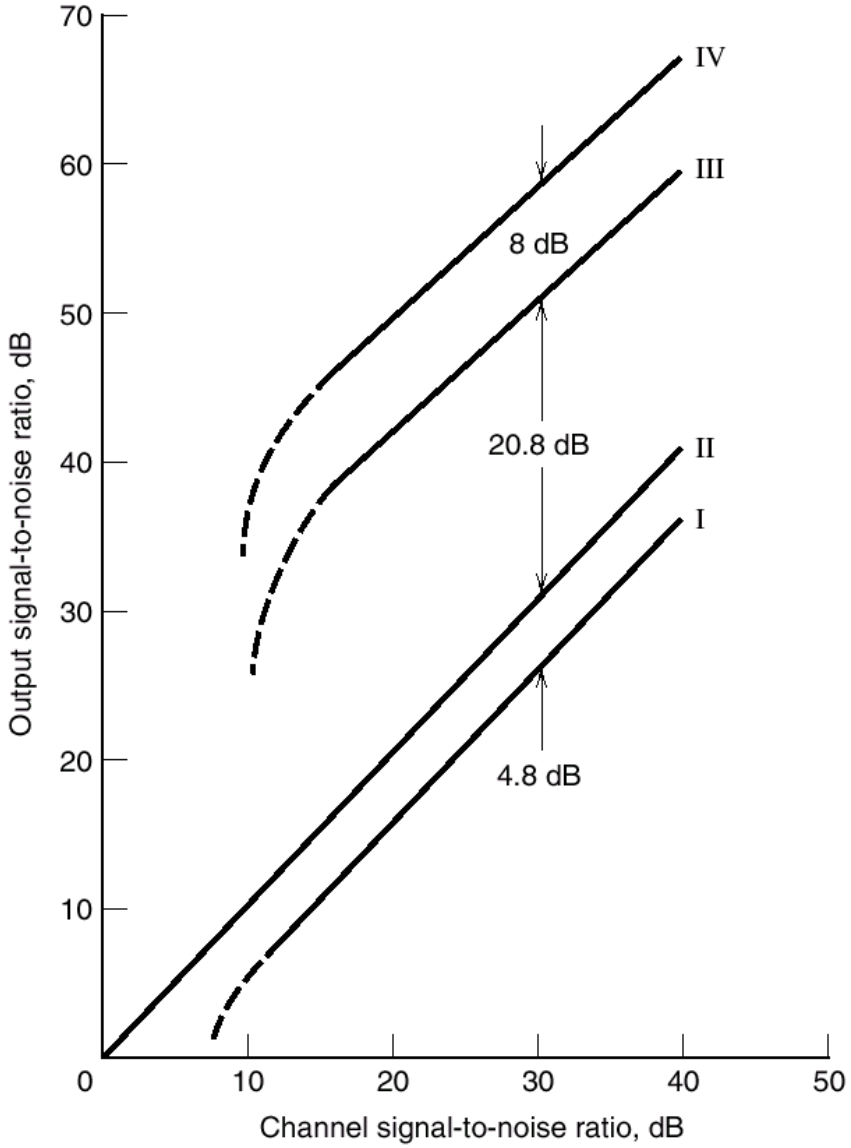


Comparison of modulation systems

Type	$b = B_T/W$	$(S/N)_D/\gamma$	γ_{th}	DC	Complexity	Comments	Typical applications
Baseband	1	1	...	No†	Minor	No modulation	Short-haul links
AM	2	$\frac{\mu^2 S_x}{1+\mu^2 S_x}$	20	No	Minor	Envelope detection $\mu \le 1$	Broadcast ratio
DSB	2	1	...	Yes	Major	Synchronous detection	Analog data, multiplexing
SSB	1	1	...	No	Moderate	Synchronous detection	Point-to-point voice, multiplexing
VSB	1+	1	...	Yes	Major	Synchronous detection	Digital data
VSB + C	1+	$\frac{\mu^2 S_x}{1+\mu^2 S_x}$	20	Yes‡	Moderate	Envelope detection $\mu < 1$	Television video
PM§	$2M(\phi_\Delta)$	$\phi_\Delta^2 S_x$	$10b$	Yes	Moderate	Phase detection $\phi_\Delta \le \pi$	Digital data
FM§¶	$2M(D)$	$3D^2 S_x$	$10b$	Yes	Moderate	Frequency detection	Broadcast radio, microwave relay, satellite systems

† Unless direct-coupled.
‡ With electronic DC restoration.
§ $b \ge 2$.
¶ Deemphasis not included.

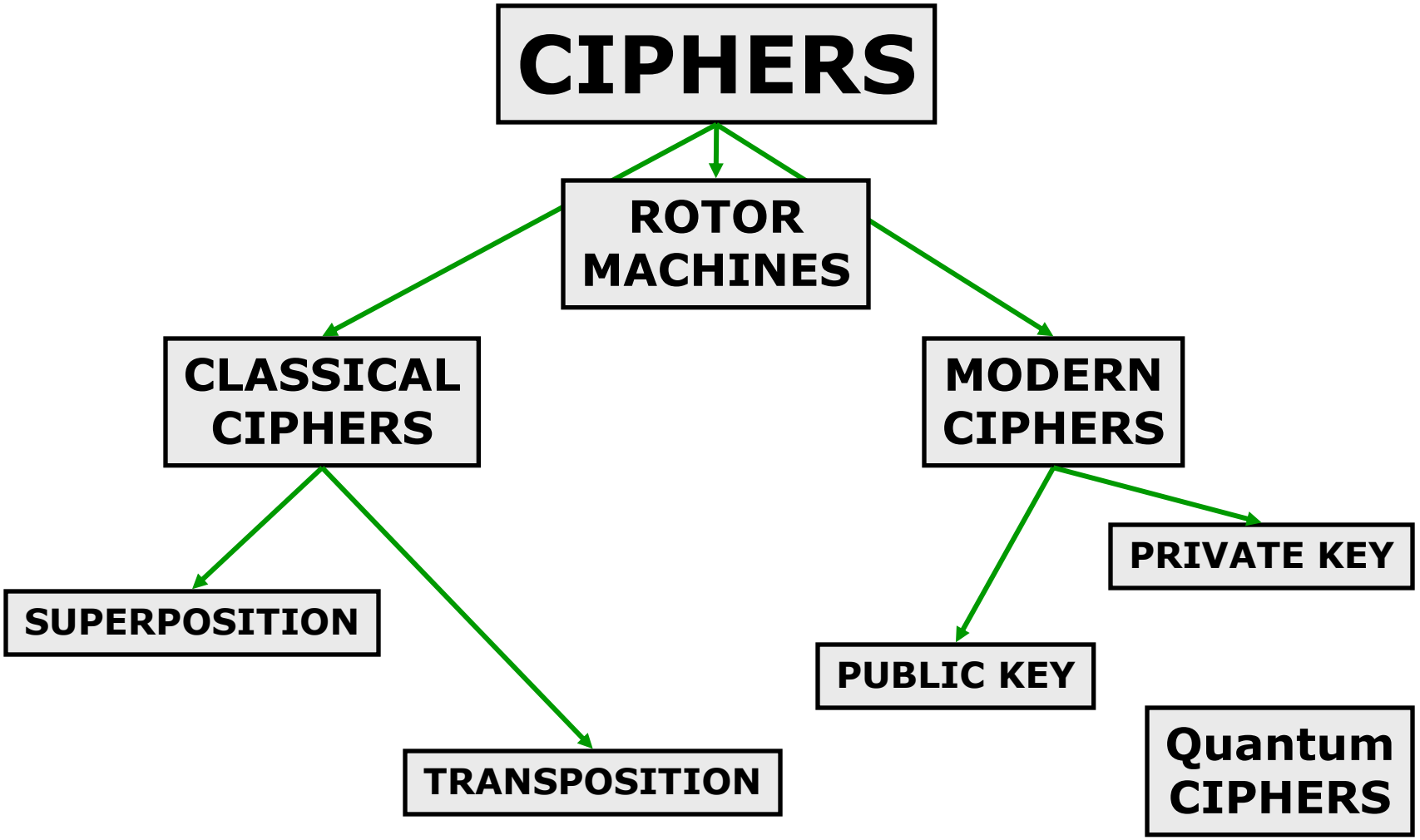
Comparison of the noise performance of various CW modulation systems. Curve I: Full AM, μ = 1. Curve II: DSB-SC, SSB. Curve III: FM, β = 2. Curve IV: FM, β = 5. (Curves III and IV include 13-dB pre-emphasis, de-emphasis improvement..)



Encryption

- **Encryption is a translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher (text).**
- **Encryption can be used to ensure secrecy, but other techniques are still needed to make communications secure: authentication, authorization, and message integrity.**
  - **Message integrity - both parties will always wish to be confident that a message has not been altered during transmission. The encryption makes it difficult for a third party to read a message, but that third party may still be able to alter it in a useful way.**
  - **Authentication is a way to ensure users are who they say they are - that the user who attempts to perform functions in a system is in fact the user who is authorized to do so.**
  - **Authorization protects computer resources (data, files, programs, devices) by allowing those resources to be used by resource consumers having been granted authority to use them.**
  - **Digital rights management etc.**

Encryption – cipher taxonomy



Transposition Method

- Da Vinci's code
- Ex.

  I am a student

  I m s u e t

  a a t d n

Substitution Method

- Shift Cipher (Caesar's Cipher)

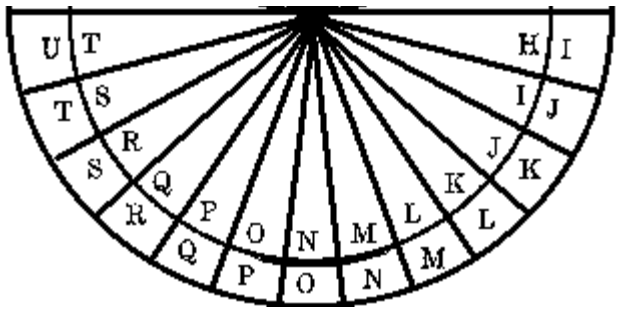
  I CAME I SAW I CONQUERED

  H BZLD H TZV H BNMPTDSDC

Julius Caesar to communicate with his army

plain ABCDEFGHIJKLMNOPQRSTUVWXYZ

cipher DKVQFIBJWPESCXHTMYAUOLRGZN



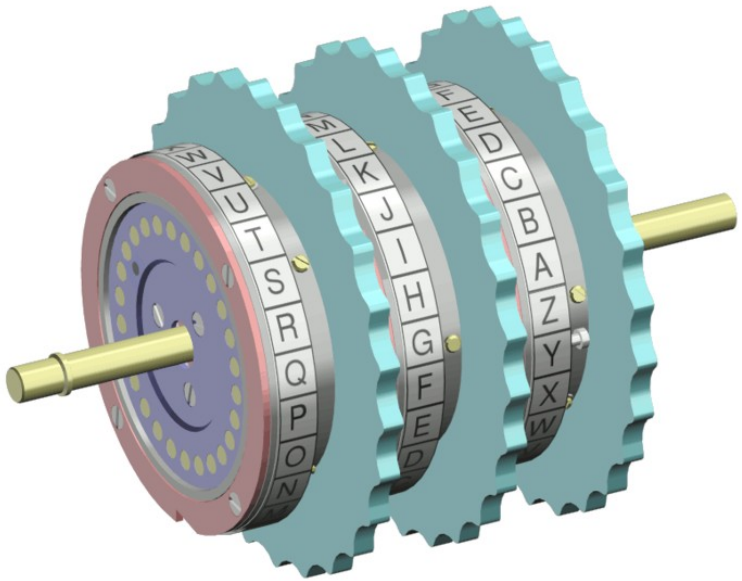
Language, wind talker

Rotor Machine

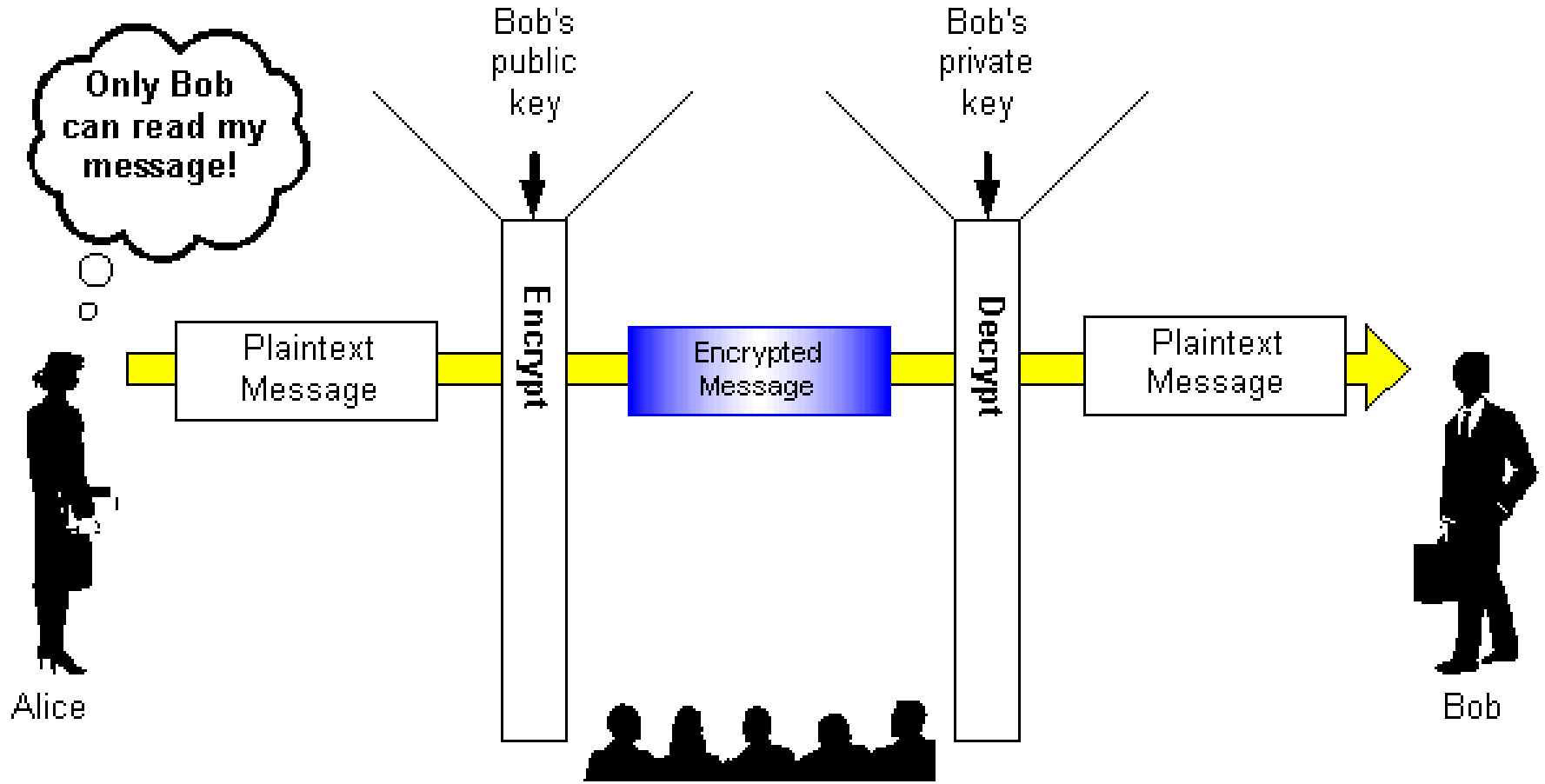
- The primary component is a set of *rotors*, also termed *wheels* or *drums*, which are rotating disks with an array of electrical contacts on either side. The wiring between the contacts implements a fixed substitution of letters, scrambling them in some complex fashion. On its own, this would offer little security; however, after encrypting each letter, the rotors advance positions, changing the substitution. By this means, a rotor machine produces a complex polyalphabetic substitution cipher.
- German Enigma machine used

during World War II for submarine.

Movie U571, Italian Job



Key


Only Bob can read my message!
Bob's public key
Bob's private key
Plaintext Message
Encrypt
Encrypted Message
Decrypt
Plaintext Message
Alice
Bob

Public Key System - RSA

- Named after its inventors Ron Rivest, Adi Shamir and Len Adleman
- Base on Number Theory

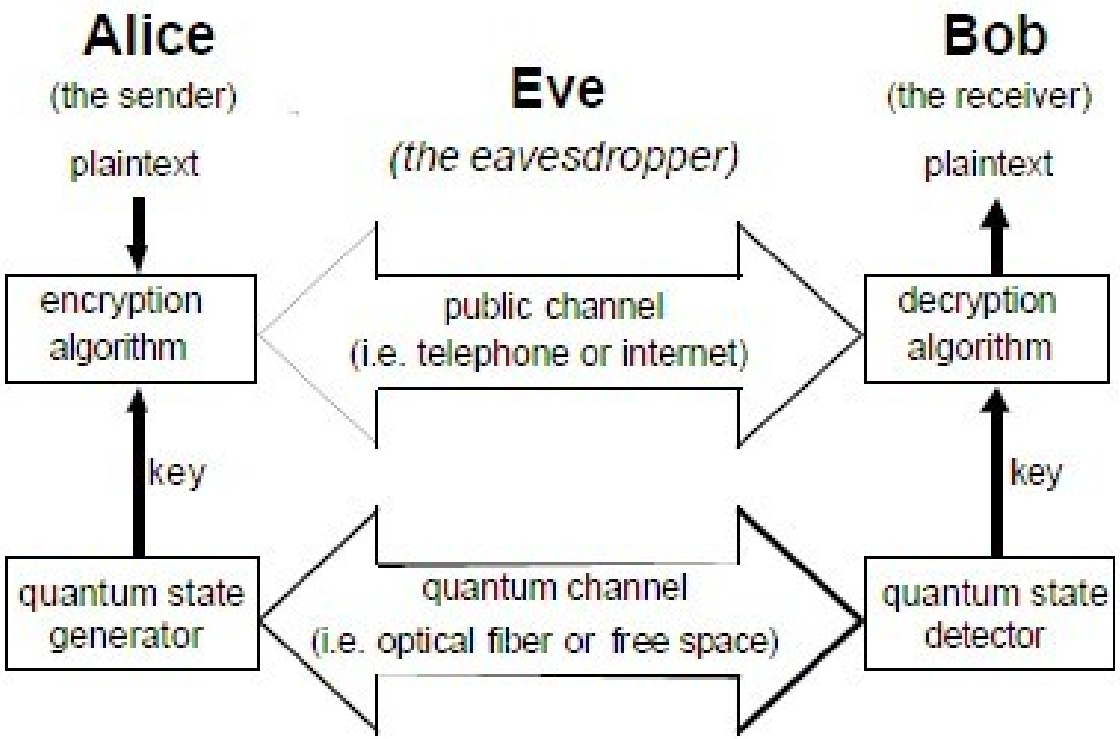
  $y=e^x \pmod N \Rightarrow x=??$
- If the size of N is 100, it takes 100 billion years to decipher with 1GHz computer.
- Applications
  - Digital Signatures
  - Digital Cash: Movie, swordfish
  - Timestamping Services: Movie, entrapment
  - Election
- Movie, mercury rising

Encryption – cipher taxonomy

- **Historical pen and paper ciphers used in the past are sometimes known as classical ciphers. They include substitution ciphers and transposition ciphers.**
- **During the early 20th century, more sophisticated machines for encryption were used, rotor machines, which were more complex than previous schemes.**
- **Encryption methods can be divided into symmetric key algorithms and asymmetric key algorithms. In a symmetric key algorithm (DES, AES), the sender and receiver must have a shared key set up in advance and kept secret from all other parties; the sender uses this key for encryption, and the receiver uses the same key for decryption.**
- **In an asymmetric key algorithm (RSA), there are two separate keys: a public key is published and enables any sender to perform encryption, while a private key is kept secret by the receiver and enables him to perform decryption.**

Quantum Cryptography

- Use physics law, if the signal is measured (eavesdropped), the receiver can always detected.



Thanking You