



**ATTEMPT  
CRYPTANALYSIS;  
INVEST \$\$\$\$\$\$\$\$**



**COMPROMISE  
ENCRYPTION  
KEYS; INVEST \$\$**

# Threats to Cryptographic Keys



All your keys  
are belongs to  
me

- ➡ Weak/Insecure generation
- ➡ Attack on transmission
- ➡ Unauthorized disclosure
- ➡ Loss