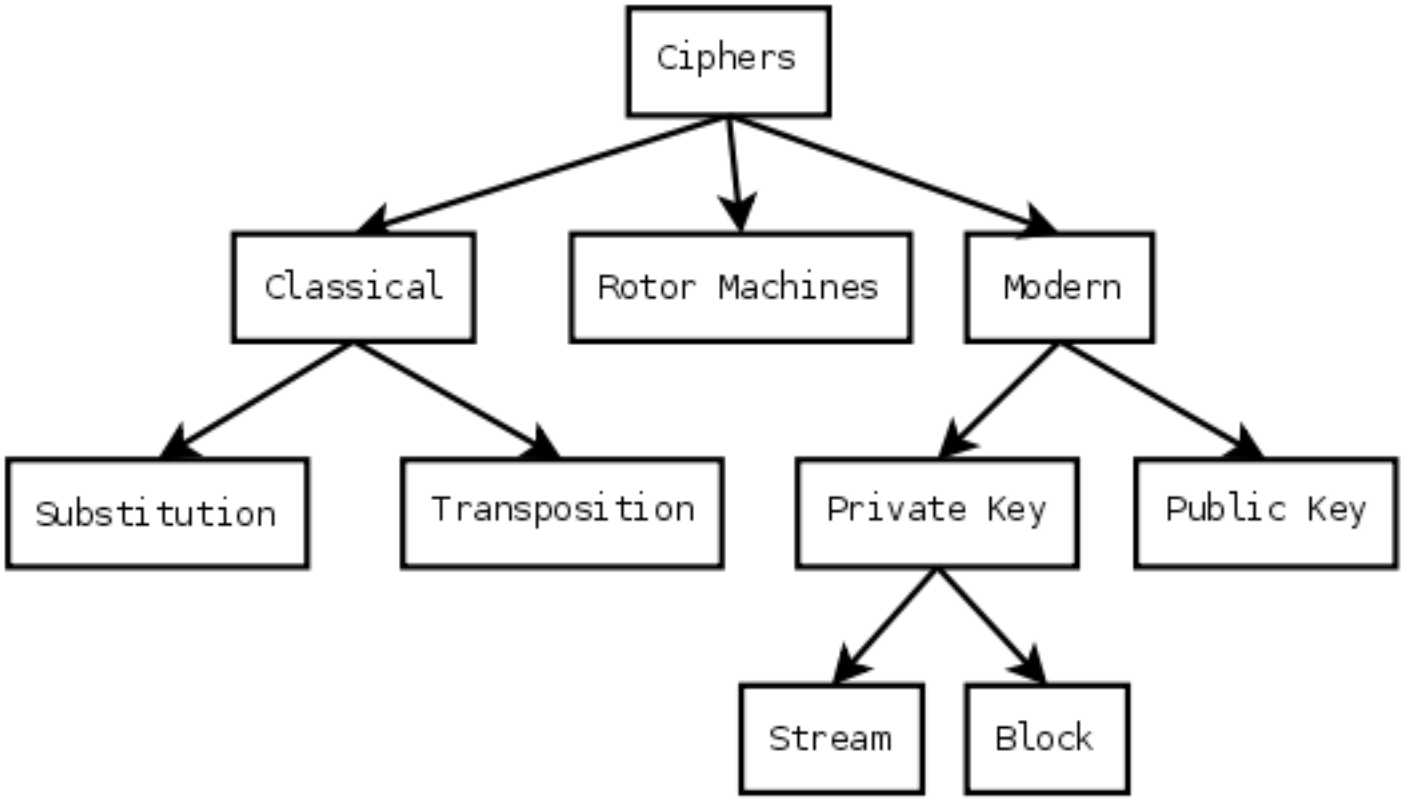
Lecture 38: crypto



order N = large prime
generator g = large prime

Alice

A=g^a mod N
B^a=g^ab mod N

publish A on her website

Bob

B=g^b mod N
A^b = g^ab mod N

C=m*(g^ab) mod N, B

ElGamal cipher

Rivest, Shamir, Adleman (RSA)