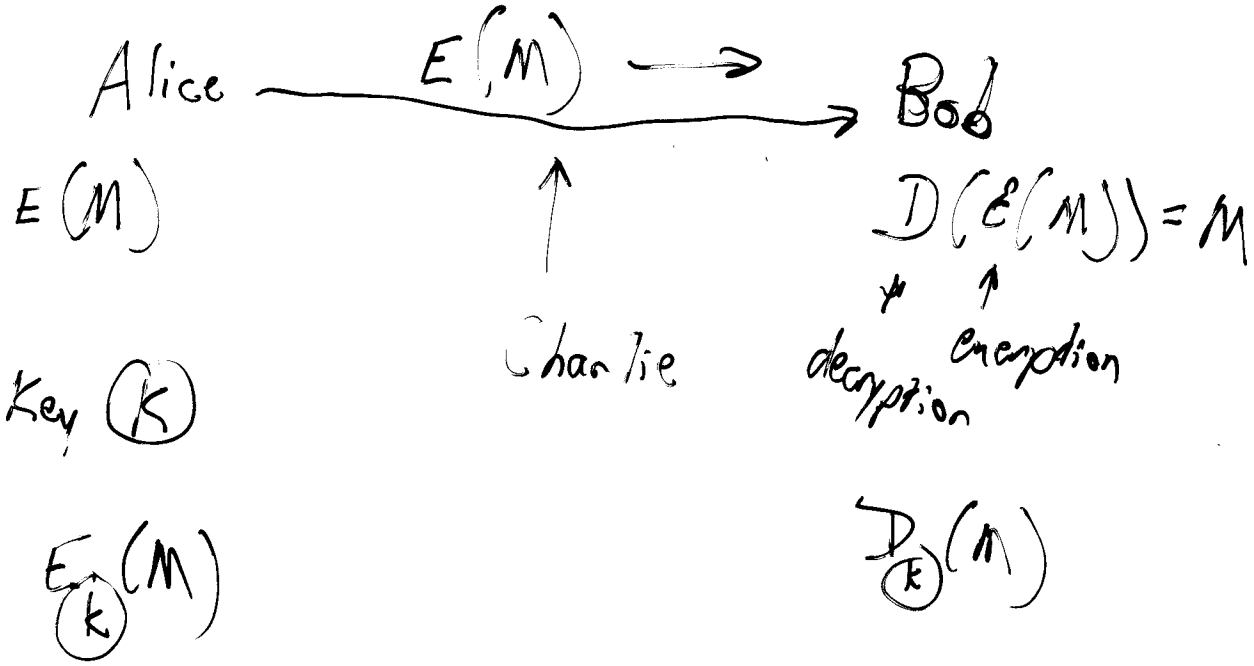
Digital Computing in the Presence of an Adversary

Cryptology / Cryptographic Protocols

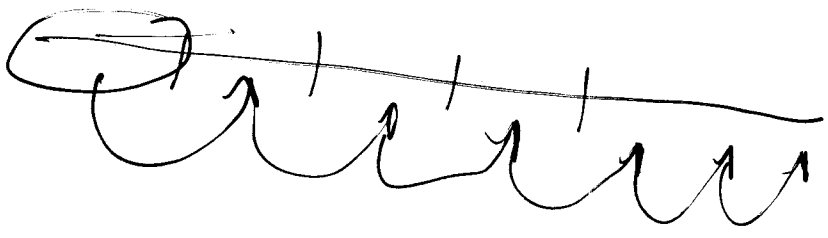
- Privacy
- Authentication
- Value Exchange
- Digital Cash
- Digital Rights Management
  - Content Protection
  - Code Protection
- Electronic Voting



One-time pad

K = "random" bit sequence 0 1 . . . . 1 1 0 0 . . . .
same length as message 1 0 0 1 1
mod2 sum = 1 1 0 0 . . . . . .

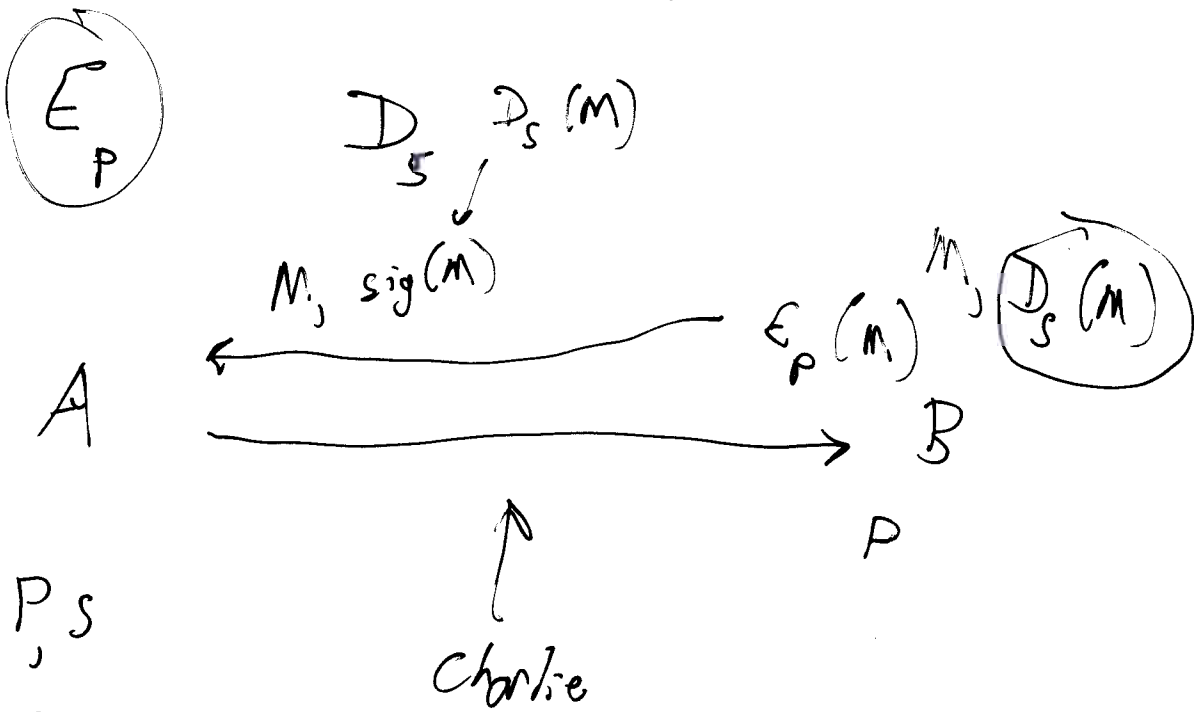
DES
↓
AES



Diffie + Hellman:

Public Key Crypto:

Two Keys: public key, private key



P, S

$D_S(E_P(M)) = M$

Trap-Door One-Way Function

Digital Signatures

RSA Cryptosystem

1. Select p, q two large primes, randomly. $n = pq$

2. Select (small) odd e relatively prime to $\phi(n) = (p-1)(q-1)$

4. Compute $d = e^{-1} \bmod \phi(n)$ via extended Euclidean algorithm

$P = (e, n)$ = Public Key

$S = (d, n)$ = Secret Key

5. $P(M) = M^e \pmod n$

$S(C) = C^d \pmod n$

} use repeated squaring

$$de = 1 + k(p-1)(q-1)$$

$$M^{de} \equiv M\left(M^{p-1}\right)^{k(q-1)} \pmod{p}$$

$$\equiv M(1)^{k(q-1)} \pmod{p} \quad \text{by Fermat's theorem:}$$

$$\equiv M \pmod{p}$$

$a^{p-1} \equiv 1 \pmod{p}$ if p is prime

Similarly,

$$M^{de} \equiv M \pmod{q}$$

$$\Rightarrow M^{de} \equiv M \pmod{pq} \quad \text{by Chinese remainder theorem}$$

Miller's Primality Test

$n \geq 1$

1. Let $n-1 = 2^e m$, m odd
2. Choose random $a \leq n-1$
3. Calculate $a^m \bmod n$. If $a^m \equiv 1 \pmod n$ halt prime
4. Calculate $a^m, a^{2m}, a^{4m}, \ldots a^{2^e m} = a^{n-1} \pmod n$ by repeated squaring. If $a^{n-1} \not\equiv 1 \pmod n$ halt composite
5. Find largest k such that $a^{2^k m} \not\equiv 1 \pmod n$. If $a^{2^k m} \equiv -1 \pmod n$ halt prime else composite

If n is prime, alg always halts prime

If n is composite, alg halts composite with prob. $\geq 1/2$