Diffie-Hellman Key Exchange: [Diffie-Hellman '76].

Very often, Alice and Bob want to agree on a key. and DES/AES.

DH Key change: allow Alice and Bob to agree on a number K in public.

Algorithm: public private

1. Alice or Bob selects a large prime p and a primitive root g of p. Both g and p are made public.
2. Alice selects a secret random $1 \le x \le p-2$.
   Bob " " " " $1 \le y \le p-2$.
3. Alice sends Bob $g^x \bmod p$.
   Bob sends Alice $g^y \bmod p$.
4. Alice and Bob both compute $K = g^{xy} \bmod p$. as the private key to agree on.

Correctness:

Alice knows x and $g^y \bmod p$.
so she can compute $(g^y)^x \bmod p$.

Bob knows y and $g^x \bmod p$.
So he can compute $(g^x)^y \bmod p$.

Security:

Eve knows: g, p, $g^x \bmod p$, $g^y \bmod p$.

To break DH Key exchange, Eve needs to compute $g^{xy} \bmod p$.

Claim. If Eve can solve discrete logs, then she can break Diffie-Hellman key exchange.

Proof: She can solve discrete logs and compute x and y, and then she can compute $g^{xy} \bmod p$.

Bit Commitment:

1. Alice wants to send Bob a bit b (either 0 or 1).
2. Bob cannot determine b without Alice's help.
3. Alice cannot change b once she sends it.

Solution:

1. They agree on a large prime $p \equiv 3 \pmod 4$ and primitive root g of p.
2. Alice choose a random $1 \leq x \leq p-2$ whose second lowest bit is b.
   She send $g^x \bmod p$ to Bob.

Correctness:

- Bob cannot compute b because he cannot solve discrete logs. (roughly speaking).
- Alice cannot change b because there is a unique x s.t $g^x \bmod p$ matches her earlier message to Bob.
- After the bet, Alice reveal x to Bob.
  Bob verifies the value of $g^x \bmod p$. and resolves the bet based on b (the second lowest bit of x).