KEY AGREEMENT

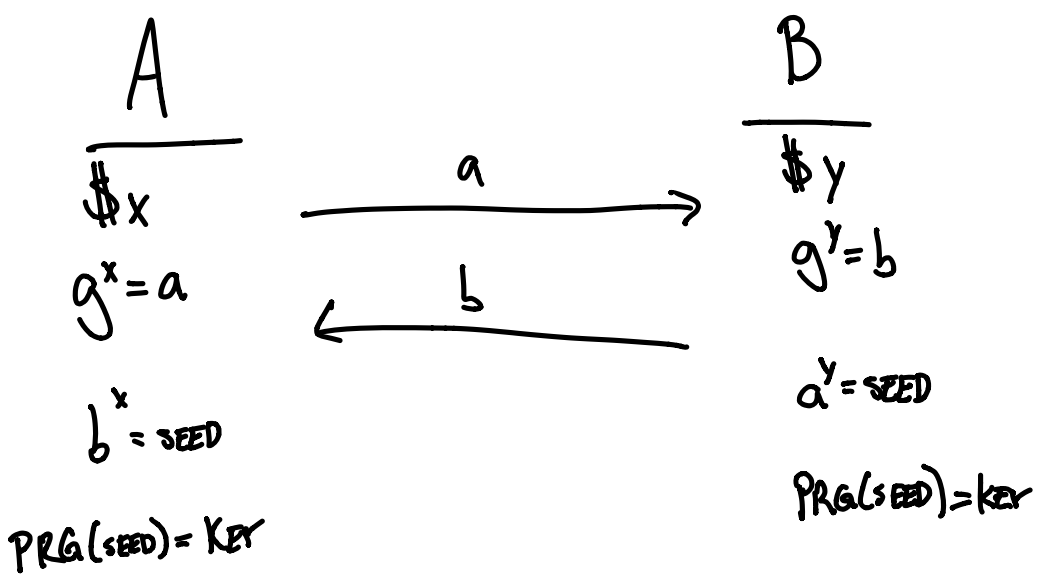
HOW TO SECURELY COMMUNICATE?

NEED TO AGREE ON SECRET KEY FOR SECURE COMMUNICATION.

DIFFIE-HELLMAN KEY EXCHANGE

BOTH KNOW $\mathbb{Z}_p$, g, PRG

g: GENERATOR



SAME KEY BECAUSE $b^x = (g^y)^x = (g^x)^y = a^y \pmod p$

WHY CAN'T AN EAVESDROPPER LEARN THE KEY?

DECISIONAL DIFFIE-HELLMAN (DDH) ASSUMPTION

THE FOLLOWING DISTRIBUTIONS ARE COMPUTATIONALLY INDISTINGUISHABLE

$$(g, g^a, g^b, g^{ab})$$

$$(g, g^a, g^b, g^r)$$

EAVESDROPPER SEES g (public), g^x, & g^y, AND MUST FIGURE OUT g^{xy} = SEED. BUT DDH TELLS US THAT FOR POLY-TIME MACHINES, THIS IS AS HARD AS FIGURING OUT g^r FOR RANDOM r. SO EAVESDROPPER LEARNS NOTHING.

NOW, WE CAN DEFINE THE NOTION OF PUBLIC KEY ENCRYPTION.

Public Key Encryption

$\text{KeyGen}(1^k, R) \longrightarrow (pk, sk)$

pk: public, sk: secret

$\text{Encrypt}(M, pk, R') \longrightarrow CT$

$\text{Decrypt}(CT, sk) \longrightarrow M$

Idea Bob can send encrypted message to Alice by encrypting under her public key. Only Alice (or anyone who learns her secret key) can decrypt.

Security Notions:

Correctness: If (pk, sk) generated honestly,

$$D(E(M, pk, R), sk) = M$$

Indistinguishability / Semantic Security: How should we define this formally?

Goldwasser/Micali answered this in paper on Probabilistic Encryption.

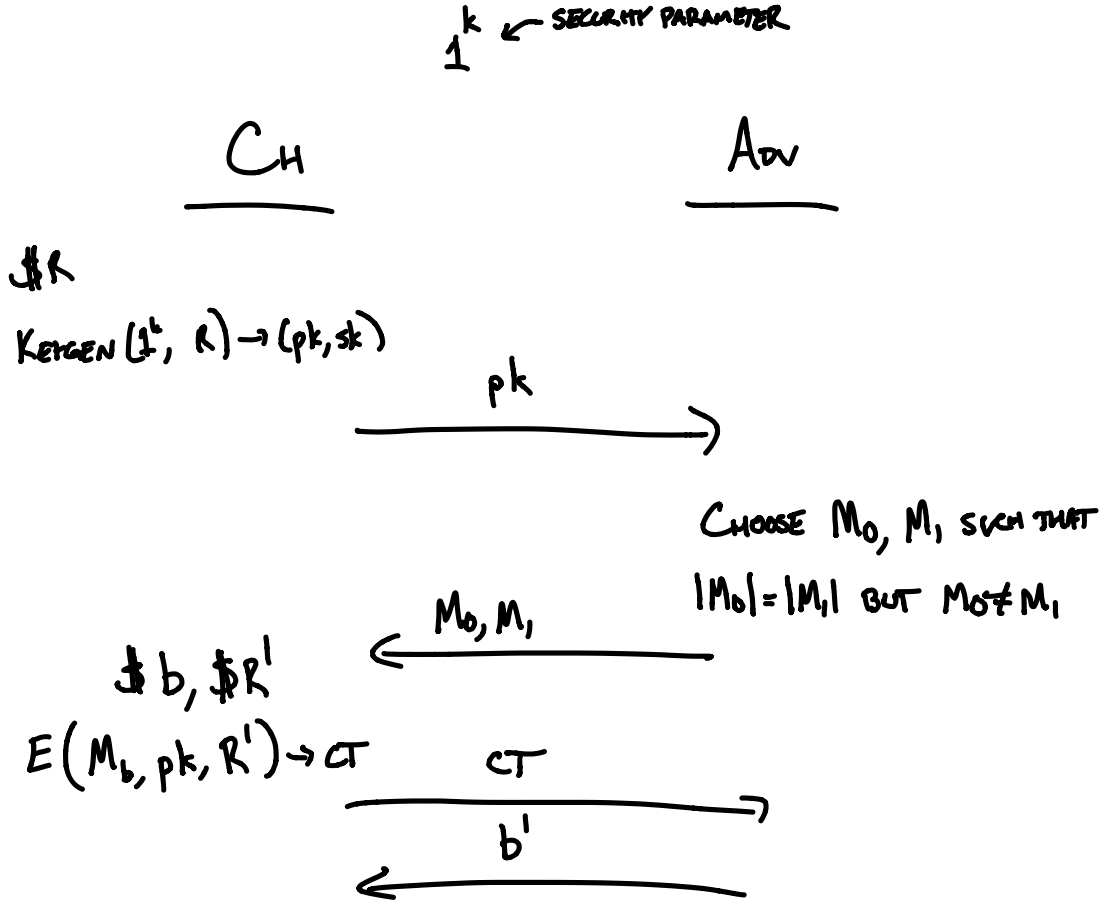
Question: Why do we need R in encryption? What if $M \longrightarrow CT$ is deterministic?

Problem: If eavesdropper knows all of M except last bit, can compute $E(M||0, pk)$ and $E(M||1, pk)$ & compare to CT, learning last bit of M.

THIS MOTIVATES OUR SECURITY DEFINITION.

EVEN IF EAVESDROPPER KNOWS ALL BUT ONE BIT OF M, SHOULD NOT BE ABLE TO GUESS REMAINING BIT EXCEPT WITH NEGLIGIBLE PROBABILITY.

DEF: INDISTINGUISHABILITY / SEMANTIC SECURITY



ADV WINS IF $b' = b$

SCHEME IS SEMANTICALLY SECURE IF $\Pr[\text{ADV WINS}] < \frac{1}{2} + \varepsilon(k)$

FOR ANY ADV $\in$ PPT AND ANY NON-NEGLIGIBLE $\varepsilon(k)$.

LET'S BUILD A PKE SCHEME!

El Gamal Encryption

sk	pk
$\$ x \in \mathbb{Z}_p$ $h \leftarrow g^x$	$\mathbb{Z}_p, g, h$

$$E(M, pk, r) = (g^r, h^r \cdot m) = CT = (u, v)$$

$$D((u,v), sk) = \frac{v}{u^x}$$

Correctness: $D(E(m, pk, r), sk) = \frac{h^r \cdot m}{(g^r)^x} = \frac{(g^x)^r \cdot m}{(g^r)^x}$

$$= m$$

Semantic Security:

Proof by contrapositive. Suppose $A \in PPT$ wins the semantic security game with probability $\frac{1}{2}+\varepsilon$ for non-negligible ε. We will show that A can be used to break the DDH assumption.

By assumption, $Pr[b'=b] = \frac{1}{2} + \varepsilon$ in the following game:

C_H		A
$\$ R$		
$KeyGen(1^\lambda, R) \to (pk, sk)$		
	$\xrightarrow{pk}$	
		Choose M_0, M_1 such that $\lvert M_0\rvert = \lvert M_1\rvert$ but $M_0 \neq M_1$
	$\xleftarrow{M_0, M_1}$	
$\$ b, \$ R'$		
$E(M_b, pk, R') \to CT$		
	$\xrightarrow{CT}$	
	$\xleftarrow{b'}$	

SUPPOSE WE ARE GIVEN

$$(g_1, g_2, g_3, g_4) = \begin{matrix} (g, g^a, g^b, g^{ab}) \\ \text{OR} \\ (g, g^a, g^b, g^r) \end{matrix}$$

HOW CAN WE USE A AS A SUBROUTINE TO DETERMINE WHICH WORLD WE ARE IN?

C_H	A_{DV}
	$\xrightarrow{pk = \mathbb{Z}_p, g_2, g_1}$
	CHOOSE M_0, M_1 SUCH THAT $\lvert M_0\rvert = \lvert M_1\rvert$ BUT $M_0 \neq M_1$
	$\xleftarrow{M_0, M_1}$
$\$ b$	
$CT \leftarrow (g_3, g_4 \cdot M_b)$	$\xrightarrow{CT}$
	$\xleftarrow{b'}$

IF $b' = b$, SAY $(g_1, g_2, g_3, g_4) = (g, g^a, g^b, g^{ab})$

IF $b' \neq b$, SAY $(g_1, g_2, g_3, g_4) = (g, g^a, g^b, g^r)$

WHY DOES THIS WORK?

CASE ANALYSIS:

IF $(g_1, g_2, g_3, g_4) = (g, g^a, g^b, g^{ab})$:

$pk = \mathbb{Z}_p, g^a, g$

$CT = (g^b, g^{ab} \cdot M_b)$

EXACTLY EL GAMAL ENCRYPTION OF M_b WITH $r = b$. THUS A PREDICTS $b' = b$ WITH PROBABILITY $\frac{1}{2} + \varepsilon$

IF $(g_1, g_2, g_3, g_4) = (g, g^a, g^b, g^r)$:

$pk = \mathbb{Z}_p, g^a, g$

$CT = (g^b, g^r \cdot M_b)$

EVEN INFINITELY POWERFUL A CANNOT PREDICT b BECAUSE $\exists\, r_0, r_1$ SUCH THAT $g^{r_0} \cdot M_0 = g^{r_1} \cdot M_1$. A DOES NOT KNOW r, SO BOTH VALUES OF b ARE EQUALLY LIKELY. THUS A PREDICTS $b' = b$ WITH ONLY PROBABILITY $\frac{1}{2}$.

THUS: $Pr[\text{PREDICT } (g_1, g_2, g_3, g_4) \text{ CORRECTLY}] =$

$$Pr[\text{PREDICT CORRECTLY} \mid (g_1, g_2, g_3, g_4) = (g, g^a, g^b, g^{ab})] \cdot Pr[(g_1, g_2, g_3, g_4) = (g, g^a, g^b, g^{ab})]$$
$$+ Pr[\text{PREDICT CORRECTLY} \mid (g_1, g_2, g_3, g_4) = (g, g^a, g^b, g^r)] \cdot Pr[(g_1, g_2, g_3, g_4) = (g, g^a, g^b, g^r)]$$
$$= \left(\frac{1}{2} + \varepsilon\right) \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2} + \frac{\varepsilon}{2}. \quad \blacksquare$$

EL GAMAL IS SEMANTICALLY SECURE!

ARE THERE ANY OTHER RELEVANT PROPERTIES?

SUPPOSE WE ENCRYPT TWO MESSAGES a + b.

$$E(a) = (g^r, h^r \cdot a)$$
$$E(b) = (g^{r'}, h^{r'} \cdot b)$$

$$E(a) \circledast E(b) = (g^{r+r'}, h^{r+r'} \cdot ab)$$

$\circledast$ = COMPONENT WISE MULTIPLICATION

VALID ENCRYPTION OF ab WITH RANDOMNESS $r+r'$

CALL THIS HOMOMORPHIC ENCRYPTION

Different flavors of homomorphic encryption:

$$E(a) \circledast E(b) = E(a * b)$$

$$E(a) \circledast E(b) = E(a \oplus b)$$

Re-randomizable encryption:

$$E(x) \rightsquigarrow E(x)$$ (new encryption w/ different randomness)

Fully Homomorphic Encryption:

$$E(a) \circledast E(b) = E(a * b)$$

and $$E(a) \oplus E(b) = E(a + b)$$

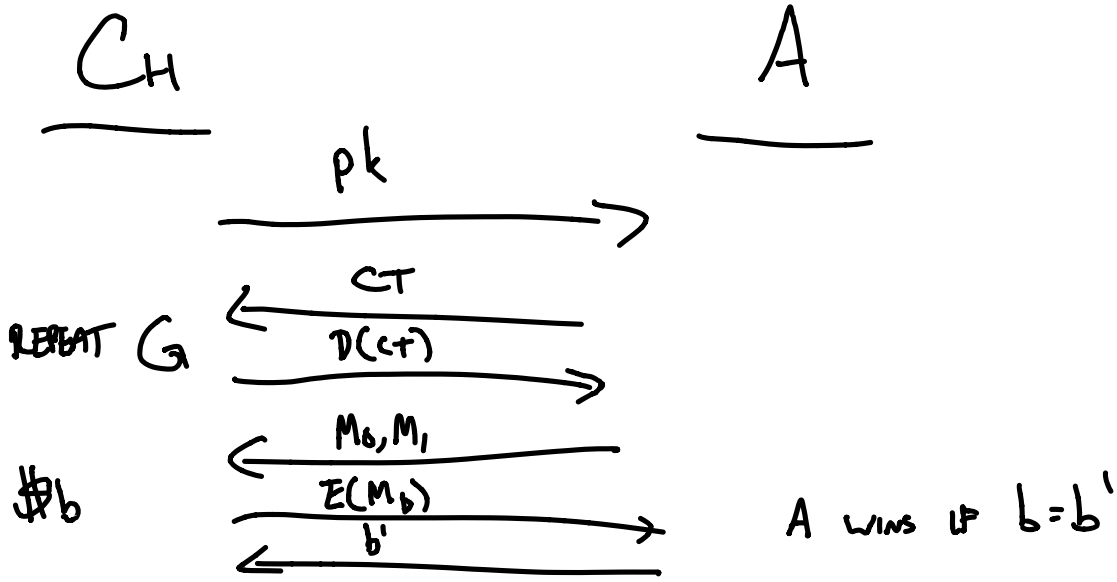
Since any circuit can be done with + and *,

FHE allows for fully secure private computation.

BUT: THERE ARE MORE EFFICIENT WAYS TO DO SECURE COMPUTATION W/O FHE.

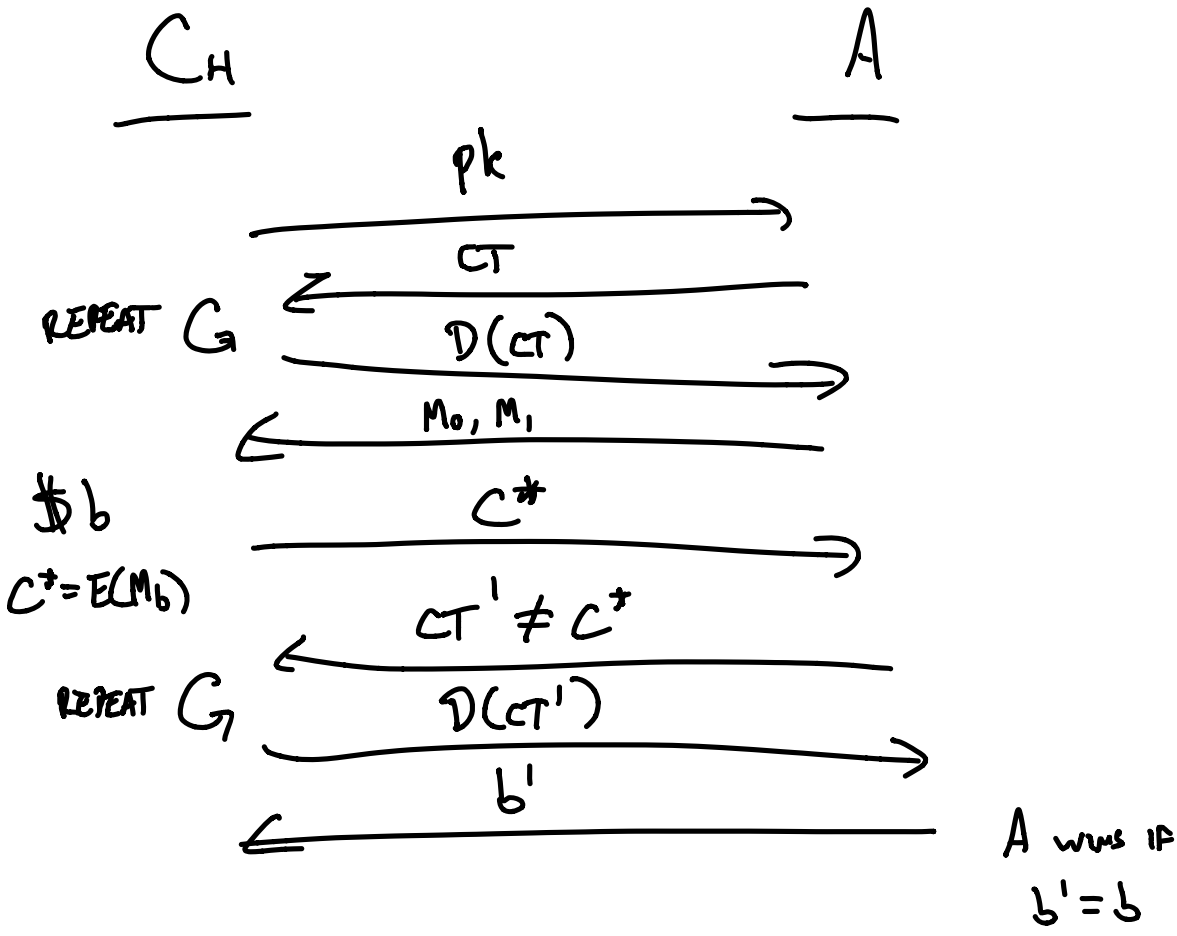
ARE THERE OTHER IMPORTANT SECURITY NOTIONS FOR ENCRYPTION?

CHOSEN CIPHERTEXT ATTACK (CCA-1)
AKA LUNCHTIME ATTACK



INTUITION: EVEN SEEING DECRYPTED CIPHERTEXTS DOESN'T HELP DISTINGUISH NEW CIPHERTEXTS.

CCA-2:



INTUITION: CCA-2 PREVENTS HOMOMORPHISM. IF $CT' = E(2 \cdot C^*)$, CAN LEARN C^*.

THIS IS CALLED NON-MALLEABILITY.