Given message independence: Prem=m/c=c] = Prem=m] Prove ciphertext independence: Prec=clm=m] = Prec=cl Using conditional probability Prec=c] = Zk Prec=c k=k] · Prek=k] applying Bayes (messem: Prec=c m=m] = Prem=m c=c] · Prec=cl Prem=m] => Prem=m c=c] · Prec=cl thus Prec=c m=m] = Prec=cl following Prec=c m=m,] = Prec=c m=m_2] Thus proving ciphertext is independent of the message text.		
Prove Ciphertext independence: Prove Ciphertext independence: Prove Ciphertext independence: Prove Cipherm = Process Prove Cipherm = Process Prove Cipherm = Process Proving Ciphertext is independent of the message text.		constitution de la desendence
Prove Ciphertext independence: Prove Ciphertext independence: Prove Ciphertext independence: Prove Cipherm] = Process Prove Cipherm] = Process Prove Cipherm] = Process Proving Ciphertext is independent of the message text.		Given message macquest
Using conditional probability P(C=c] = Zk P(C=c k=k] P(C=c k=k] Applying Bayes (mearem: P(C=c M=m] = P(M=m C=c] P(C=c] P(C=c M=m] = P(C=c] P(C=c M=m] = P(C=c] Thus P(C=c M=m] = P(C=c M=m,] = P(C=c M=m] Thus proving cipnestext is independent of the message text.		
Using conditional probability P(C=c] = Zk P(C=c k=k] P(C=c k=k] Applying Bayes (mearem: P(C=c M=m] = P(C=c] P(C=c] P(C=c M=m] = P(C=c] P(C=c M=m] = P(C=c] thus P(C=c M=m] = P(C=c] following P(C=c M=m,] = P(C=c M=m_z) Thus proving (ignestext is independent of the message text.		1 de Den dence
Using conditional probability P(C=c] = Zk P(C=c k=k] P(C=c k=k] Applying Bayes (mearem: P(C=c M=m] = P(C=c] P(C=c] P(C=c M=m] = P(C=c] P(C=c M=m] = P(C=c] thus P(C=c M=m] = P(C=c] following P(C=c M=m,] = P(C=c M=m_z) Thus proving (ignestext is independent of the message text.		Prove Ciphertext indeportation
applying Bayes (mearem: Pr[C=c[M=m]= Pr[M=m]C=c] Pr[M=m] => Pr[M=m]Q=c] Pr[C=c] Pr[M=m]C=c] thus Pr[C=c[M=m] = Pr[C=c] following Pr[C=c[M=m,]= PrEc=c[M=m] Thus proving cipnestext is independent of the message text.	/	PCC=CLW=W] = PCCC-CI
applying Bayes (mearem: Pr[C=c M=m]= Pr[M=m C=c] Pr[M=m] => Pr[M=m Q=c] Pr[C=c] Pr[M=m C=c] thus Pr[C=c M=m] = Pr[C=c] following Pr[C=c M=m,]= Pr[c=c M=m] Thus proving cipnettext is independent of the message text.		
applying Bayes (mearem: Pr[C=c[M=m]= Pr[M=m]C=c] Pr[M=m] => Pr[M=m]Q=c] Pr[C=c] Pr[M=m]C=c] thus Pr[C=c[M=m] = Pr[C=c] following Pr[C=c[M=m,]= PrEc=c[M=m] Thus proving cipnestext is independent of the message text.		Using conditional probability
applying Bayes (mearem: Pr[C=c[M=m]= Pr[M=m]C=c] Pr[M=m] => Pr[M=m]Q=c] Pr[C=c] Pr[M=m]C=c] thus Pr[C=c[M=m] = Pr[C=c] following Pr[C=c[M=m,]= PrEc=c[M=m] Thus proving cipnestext is independent of the message text.		bulled = 5 kullich kirk 1. Aulk = k]
Pr[C=c M=m] = Pr[M=m C=c]. Pr[C=c] Pr[M=m]		
Pr[C=c M=m] = Pr[M=m C=c]. Pr[C=c] Pr[M=m]		applying Bayes encorem:
Pr[M=m Q=c]. Pr[C=c] Pr[M=m C=c] Pr[C=c M=m] = Pr[C=c] following Pr[C=c M=m,] = Pr[c=c M=m_2] Thus proving cipnertext is independent of the message text.		
Pr[M=m Q=c]. Pr[C=c] Pr[M=m C=c] Pr[C=c M=m] = Pr[C=c] following Pr[C=c M=m,] = Pr[c=c M=m_2] Thus proving cipnertext is independent of the message text.		Pr[C=c M=m]= Pr[M=m C=c] ProlC=c]
Pr[M=m Q=c]. Pr[C=c] Pr[M=m C=c] thus Pr[C=c M=m] = Pr[C=c] following Pr[C=c M=m,] = Pr[c=c M=m_2] Thus proving cipnertext is independent of the message text.		Fm=m]
thus Pr[c=c M=m] = Pr[c=c] following Pr[c=c M=m,] = Pr[c=c M=m_2] Thus proving cipnestext is independent of the message text.		
thus Pr[c=c M=m] = Pr[c=c] following Pr[c=c M=m,] = Pr[c=c M=m_2] Thus proving cipnestext is independent of the message text.		=> Pr[M=m Q=c]. Pr[c=c]
thus Pr[c=c M=m] = Pr[c=c] following Pr[c=c M=m,] = Pr[c=c M=m_2] Thus proving cipnestext is independent of the message text.		Pr[N=m/L=c]
following Pr[c=c M=m,]=Pr[c=c M=m2] Thus proving cipnestext is independent of the message text.		
following Pr[c=c M=m,]=Pr[c=c M=m2] Thus proving cipnestext is independent of the message text.		thus ,
following Pr[c=c M=m,]=Pr[c=c M=m2] Thus proving cipnestext is independent of the message text.		Pr[c=c M=m] = Pr[c=c]
Thus proving cipnestext is independent of the message text.		
Thus proving cipnestext is independent of the message text.		following
Thus proving cipnestext is independent of the message text.	grand to deligate the deligate the second of	Pr[c=c M=m.] = Pr[c=c M=m2]
		Thus proving connectent is independent of
	an a programme of the Phillippe of the American Administration	the mescage text
		The same of the sa
$A \iff K$	-4114	A ⇔ 8
$A \longrightarrow R$		
7 7		7 7
	May be now desired	
	and the second s	Andrew Control of the

	Following the neviously given cirenectext:
	Following the previously given cipnertext; PrIC=c M=m, J=PrIC=c M=m, J=PrIC=cJ
	Prove Perfect adversarial indistinguishability:
/	PrEprivKAT = 1] = 1 (215
	C=Enck(mb)
	be 80,13 given two messages
	· Chusin & 1
	P([b'=b]=1/2
1,	
	2 = Pr[priv KAT=1]
	=> Pr[c=c M=m,]. Pr[M=m,]+ Pr[C=c M=m,]. Pr[M=m,] =>
	Prcc=c M=m, J. PrcM=m2] =>
	Pr[b'=b] = Pr[b'=b b=0] · Pr[b=0] +
	Pr[P=9]04. [1=9/9=,9]3
	Pr[b'=b] = (('12)('12)) + (('12)('12))
	Pr[b'=b] = (' 4) + (' 4) = 2 4 = 1 2 = Pr[priv Kon = 1]
	= 2/4 = 1/2 = PC[Priv Kan = 1]
	7,1
	Thus,
	An adversary Cannot distinguish between
	two enclypted messages better than
	two encrypted messages better than random guessing.
	Jesung
	A ->B
	
	C D

	Given: P.A.I
	PrivkAT=1] = 1/2
and processing and the same of	Prove perfect secrety:
	tr Lenck m)=C,] = Pr [enc(k, m2) = C]
	Prcenck m)=C,]=Prcenc(k,m2)=C] = Prcc= a M=M,]=Prcc= l M=m2]
-/	_ h3a =
/	Pr[priv KA, T = 1] = Pr[C=C M=M, 7 . Pr[M=m,]+
	Prec= c= M= m2] . Prem= m2] =
-	<u> </u>
-}	>> Pr[L=c M=m,]. 12 + Pr[C=c M=m2]. 1/2 Since pr[b=b]= x x x x x x x x x
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
_/	Since 1/20 6= 107= 105
	> Pr C = C M=m, = C= L M=m2] = 1/2
	thus,
	(P([enc(k,m,)=C] = P([enc(k,m2)=C]) = 1/2
	(Canc(Mm ₂)-C) - 1/L
	being adjection lauving no adjustice
	being advectory having no advantage as both messages have a 1/2 probability tollowing P.A.I. proving perfect secrecy is equiry and to P.A.I.
	proving perfect secrecy is early user to P.A.T.
	$A \rightarrow B$
	C → D

-	Luna chert sources:
-	PCEC=C M=m, I = Pr[C=C M=vnz] = Pr[C=C]
_	ACTC-CLW-III' 7 - LLCC
-	Prove mossens independance
	Prove message independance Pr[M=m](=c] = Pr[N=m]
_	ALT WEMICACT - LICENTIA
_	1 1 m°
_	again, substituting bayes Theorem:
_	
	Pr[M=m]C=c] = Pr[C=c M=m]. Pr[M=m]
	Lo=221d
	Pr[M=m]C=C]=Pr[C=Q.Pr[M=m]
	predect
	Pr[m=m] C= C] = Pr[M=m]
	Yhus,
	unt unive showing perfect sorreus
	equivalent to message independence, but also equivalent to hipter independence, os we applied that definition area.
_	also equivalent to lighter independence
	the applied that regulation are
	as we applied that deplication and
	A
- Navingel	
	c —— N

Extra unrelated notes!!!!:

	Reflexive OtP Symmetric Ogta + politich = C+x+ Transitive (110 UbV; 1:01
	Assume Perfect Secrety:
- Ke	effect secrecy is the condition where the
1	probability distribution of a message M= m given a circumstant C=c is independent of the expertext. This means the
(iphatext ævenis no information about the meskage.
+	PrIenc(k,m.)= C]=Pr[enc(k,m)=C]
1	price of the contract of the c
+0	where AMEM, ACEC Where PULC=C]>0
	Mc Sage independence (Shannon Scircus)
1	ue want to show;
1	Pr[M=m C=c] = Pr[M=m], cipnertext proves no
	nust be independent. The encryption algorithm generates apper text uniformally lot equal distribution).
1 9	R(C·C) = Ex Pr[C=C n K=1c]
	Pr[c=onk=k]=Pr[M=c+kn k=k]
1	= Pr[M=C1 K] P[K=K]
+	= P([M= C+K] (1/N)
W	be know k runs through all possible keys.
1	C+K runs through all possible messages
	ExPr[M=C+K] = Pr[M= sime possible metrage] = 1
P	([(=c] = Epr[c=c] k=k] = ('IN) E Rr[m= c+k=)IN
+	CTRETIA

	1.05 1 7-057
	A: Pr[M=m c=c]= Pr[M=m]
	Pr[M=m]c=c] = Pr[c=c M=m]Pr[M=m].
	6676367
	23/1
Ve	(Premary Premary Premary Premary Premary
a.	Pregety offer
W	
B:	Pr[c=c] = Pr[c=c M=m]
4	=> Pr[C=C] = Pr[C=c] Pr[M=M]
	[m=m] = 1
100	a realization to the second se
C:	Precio Min] = Tal
	1. 2. 3. 3. 3. 3. 3. 3. 3. 3. 3. 3. 3. 3. 3.
La	PrEC= 1 = PrEM=m]
A 1 12	Pr[c=c] = 101 mem Pr[m-m]
	Pr[c=c] = Tot mem Pr[m-m]

	WES: (AUB) NG = (ANC) U(BNC)
	Set A = \(\{ 1, 2, 3\} \) Set B = \(\{ 2, 3, 4 \} \) Set C = \(\{ 3, 4, 6 \} \)
*:-	(AUB) MC: (AUB) = \(\xi,2,3\}U\{2,3,4\}=\xi,2,3,4\}
8.	(AUB) (C = \(\frac{2}{1},2,3,4\)\(\frac{2}{3},4,5\)\(\frac{2}{3},4\)\(\fra
	$(A \cap C) = \{3\}$ $(B \cap C) = \{3,4\}$ $(A \cap C) \cup (B \cap C) = \{3,4\} \cup \{3,4\} = \{3,4\}$
	(ANB