Cryptography

Monte Carlo Random Walk

Bashar Karaja

[1]Phys 222 Final Project

December 17, 2022

Table of Contents

Table of Contents

Sample frame title

Cryptography is a method used to protect, encode and hide certain desired data using a specific method of encryption. One of the famous, well-known encryption decryption methods is the beautiful Morse Code, which uses dots and dashes to symbolize each character.

To decrypt a text

To decrypt a text
You need to know the encryption key first

To decrypt a text
You need to know the encryption key first
But what happens when we lose this encryption key? or we don't know it from the very beginning? in other words, can we figure out the decryption key without having acess to it?

Table of Contents

Monte Carlo

For such situations, Monte Carlo comes to be of great importance, but What is Monte Carlo Random Walk?

Definition

a broad class of computational algorithms that rely on repeated random sampling to obtain numerical results

Usage

Monte Carlo methods are mainly used in three problem classes:[1] optimization, numerical integration, and generating draws from a probability distribution

Our goal

use Monte Carlo as a method for the probability distribution of character transitions, and in the encryption-decryption process.

Table of Contents

Sample frame title

a technique for random sampling from the possible state spaces in such a way that it will efficiently converge to the correct decryption. for each successive pair of characters(c1,c2), the expression r(c1,c2) records the number of times each particular pair of characters appears in the reference text we are using. similarly, we denote f(x)(c1,c2) to record the number of times each two-letter pair occurs in the target text after it was decrypted with key x from the state space

General Formula

$$\pi(x) = \prod_{c_1,c_2} r(c_1, c_2)^{f_x(c_1,c_2)}$$

Table of Contents

Metropolis Algorithm

After calculating a weight for the decryption key, a proposal key is generated by randomly choosing two letters from the key and swapping their positions. So if B and X are randomly chosen and B is mapped to E and x mapped to Y, then in the proposed key, B maps to Y and G maps to E. Then:

General Formula

First, encrypt the text by using a random encryption key.

General Formula

Calculate the weight of the decryption key

General Formula

Propose a random key by swapping two randomly chosen letters from the key

General Formula

find the weight of the proposed key

General Formula

if its ratio over the old one is greater than a randomly selected number from the interval[0,1], accept it

General Formula

otherwise, reject the guess and continue iterating

Table of Contents

I have chosen the length of the text we want to get our transition probabilities as 400,000 words or approximately 1,000,000 letters since most of the probabilities almost don't change no matter how larger the length of the text is after that(equilibrium state almost reached)
I have used other 8 texts to randomly encrypt, find the weights and then decrypt, and while it seems to be not enough, I was able to reach the full and correct guess of the 26 letters twice. Also, it took more than 2 hours to process them, so it is time-consuming to use more.

Table of Contents

alphabets	a	b	c	d	e	f	g	h	i	j	...	q	r	s	t	u	v	w
a	0.00000	0.02467	0.06086	0.05263	0.00000	0.01151	0.00987	0.00164	0.01974	0.00164	...	0.0	0.13158	0.08553	0.10855	0.00658	0.03454	0.0098
b	0.08065	0.00000	0.00000	0.00000	0.38710	0.00000	0.00000	0.00000	0.03226	0.00000	...	0.0	0.04839	0.04839	0.00000	0.04839	0.00000	0.0000
c	0.08811	0.00000	0.01762	0.00000	0.22467	0.00000	0.00000	0.18502	0.07489	0.00000	...	0.0	0.03524	0.00441	0.07048	0.04846	0.00000	0.0000
d	0.07424	0.00000	0.00000	0.04367	0.28821	0.00000	0.00000	0.00000	0.12664	0.00437	...	0.0	0.04803	0.01310	0.00000	0.01310	0.00000	0.0000
e	0.08180	0.00346	0.01498	0.03687	0.01382	0.00806	0.00461	0.00230	0.01959	0.00000	...	0.0	0.09793	0.14286	0.01843	0.00000	0.00922	0.0057
f	0.15152	0.00000	0.00000	0.00000	0.15909	0.06061	0.00000	0.00000	0.08333	0.00000	...	0.0	0.02273	0.00758	0.03788	0.03788	0.00000	0.0000
g	0.02055	0.00000	0.00000	0.00000	0.08219	0.00000	0.00685	0.20548	0.06164	0.00000	...	0.0	0.04110	0.01370	0.00000	0.01370	0.00000	0.0000
h	0.14516	0.00000	0.00000	0.00000	0.42857	0.00000	0.00000	0.00000	0.08295	0.00000	...	0.0	0.02995	0.00000	0.02074	0.00000	0.00000	0.0000
i	0.02893	0.01085	0.08318	0.02532	0.05063	0.01989	0.02532	0.00000	0.00000	0.00000	...	0.0	0.02893	0.09403	0.14105	0.00000	0.05425	0.0000
j	0.21429	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	...	0.0	0.00000	0.00000	0.00000	0.35714	0.00000	0.0000
k	0.00000	0.00000	0.00000	0.00000	0.33333	0.00000	0.00000	0.00000	0.06667	0.00000	...	0.0	0.00000	0.00000	0.00000	0.00000	0.00000	0.0000
l	0.04360	0.02035	0.00000	0.03488	0.14244	0.00291	0.00000	0.00291	0.09884	0.00000	...	0.0	0.00000	0.01744	0.13372	0.01163	0.00291	0.0000
m	0.04494	0.00000	0.00000	0.00000	0.42697	0.00000	0.00000	0.00000	0.08989	0.00000	...	0.0	0.00000	0.05056	0.00000	0.02809	0.00000	0.0000
n	0.03145	0.00000	0.05451	0.11321	0.04822	0.00839	0.17820	0.00000	0.06499	0.00000	...	0.0	0.00000	0.03983	0.24109	0.00000	0.00210	0.0000
o	0.00928	0.00928	0.01160	0.00000	0.00000	0.09049	0.01856	0.00000	0.01624	0.00000	...	0.0	0.13457	0.02784	0.03480	0.18329	0.02320	0.0510
p	0.19863	0.00000	0.00000	0.00000	0.06164	0.00000	0.00000	0.01370	0.05479	0.00000	...	0.0	0.17123	0.03425	0.02740	0.02055	0.00000	0.0000
q	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	...	0.0	0.00000	0.00000	0.14286	0.85714	0.00000	0.0000
r	0.04534	0.00000	0.04786	0.01511	0.24937	0.00000	0.00252	0.00000	0.05793	0.00000	...	0.0	0.00504	0.11083	0.11839	0.02015	0.00504	0.0000
s	0.01947	0.00000	0.01062	0.00000	0.06372	0.00177	0.00000	0.02124	0.08496	0.00000	...	0.0	0.00000	0.08673	0.14336	0.04956	0.00000	0.0070
t	0.10080	0.00000	0.00000	0.00133	0.05836	0.00000	0.00000	0.30637	0.10875	0.00000	...	0.0	0.01989	0.05703	0.00000	0.04244	0.00000	0.0000
u	0.00429	0.01717	0.06009	0.14163	0.06009	0.00858	0.08155	0.00000	0.01288	0.00000	...	0.0	0.12446	0.07296	0.07725	0.00000	0.00000	0.0000
v	0.05063	0.00000	0.00000	0.00000	0.69620	0.00000	0.00000	0.00000	0.18987	0.00000	...	0.0	0.00000	0.00000	0.00000	0.00000	0.00000	0.0000
w	0.22115	0.00000	0.00000	0.00000	0.19231	0.00000	0.00000	0.19231	0.17308	0.00000	...	0.0	0.00000	0.01923	0.00000	0.00000	0.00000	0.0000
x	0.08333	0.00000	0.00000	0.00000	0.08333	0.00000	0.00000	0.08333	0.08333	0.00000	...	0.0	0.00000	0.00000	0.00000	0.00000	0.00000	0.0000
y	0.00000	0.00000	0.02041	0.00000	0.06122	0.00000	0.00000	0.00000	0.00000	0.00000	...	0.0	0.01020	0.08163	0.00000	0.00000	0.00000	0.0000
z	0.00000	0.00000	0.00000	0.00000	0.40000	0.00000	0.00000	0.00000	0.60000	0.00000	...	0.0	0.00000	0.00000	0.00000	0.00000	0.00000	0.0000

Figure: Probability of transitions for 1000 words text.

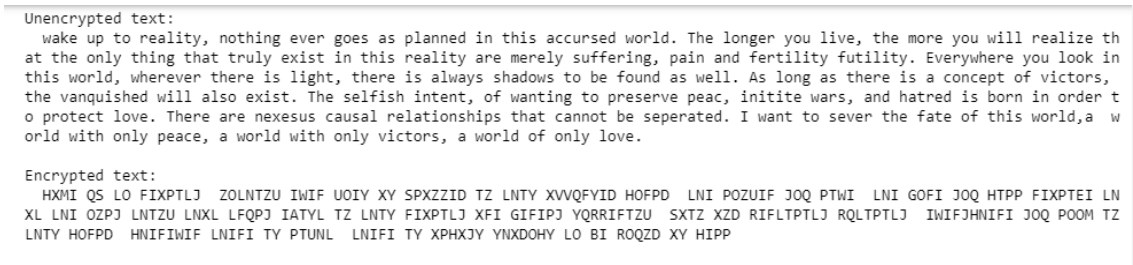
bets	a	b	c	d	e	f	g	h	i	j	...	q	r	s	t	u	v	w
a	0.00016	0.02276	0.03584	0.05044	0.00058	0.00718	0.01562	0.00222	0.04256	0.00042	...	0.00007	0.09046	0.09644	0.13772	0.01023	0.02101	0.00899
b	0.08076	0.00494	0.00000	0.00126	0.32797	0.00000	0.00000	0.00021	0.03649	0.01052	...	0.00000	0.06088	0.02639	0.00673	0.14648	0.00358	0.00000
c	0.12343	0.00000	0.01381	0.00017	0.18372	0.00000	0.00006	0.17496	0.06865	0.00000	...	0.00261	0.03319	0.00470	0.07822	0.03128	0.00000	0.00000
d	0.02641	0.00065	0.00007	0.01121	0.11357	0.00083	0.00393	0.00169	0.07873	0.00036	...	0.00014	0.02666	0.02508	0.00083	0.01286	0.00216	0.00054
e	0.04258	0.00145	0.02100	0.07141	0.02529	0.00875	0.00658	0.00217	0.01114	0.00036	...	0.00171	0.14016	0.07354	0.02730	0.00094	0.02625	0.00734
f	0.07719	0.00021	0.00056	0.00049	0.10498	0.04857	0.00021	0.00007	0.07198	0.00014	...	0.00000	0.07149	0.00208	0.03286	0.04461	0.00000	0.00007
g	0.05649	0.00015	0.00007	0.00029	0.11422	0.00007	0.00864	0.12177	0.05642	0.00000	...	0.00000	0.05250	0.01808	0.00232	0.02251	0.00000	0.00051
h	0.16135	0.00037	0.00016	0.00023	0.45690	0.00058	0.00000	0.00005	0.14581	0.00000	...	0.00000	0.00838	0.00233	0.02597	0.01231	0.00051	0.00033
i	0.01871	0.00846	0.05000	0.04498	0.03606	0.02214	0.02460	0.00064	0.00034	0.00014	...	0.00038	0.03016	0.12818	0.14416	0.00054	0.02675	0.00000
j	0.04688	0.00000	0.00000	0.00000	0.29545	0.00000	0.00000	0.00000	0.00426	0.00000	...	0.00000	0.00000	0.00000	0.00000	0.40483	0.00000	0.00000
k	0.09130	0.00069	0.00017	0.00000	0.25095	0.00035	0.00069	0.00052	0.17380	0.00000	...	0.00000	0.00328	0.02192	0.00052	0.00242	0.00000	0.00293
l	0.07444	0.00131	0.00066	0.05891	0.16915	0.02515	0.00098	0.00029	0.12252	0.00000	...	0.00000	0.00386	0.01732	0.02523	0.01917	0.00510	0.00685
m	0.15817	0.01729	0.00025	0.00000	0.25423	0.00183	0.00000	0.00019	0.10080	0.00000	...	0.00000	0.00114	0.03503	0.00057	0.03541	0.00000	0.00006
n	0.02659	0.00045	0.04040	0.16827	0.07552	0.00529	0.13713	0.00126	0.03087	0.00091	...	0.00105	0.00037	0.05043	0.09940	0.00486	0.00461	0.00070
o	0.00517	0.00782	0.01109	0.01475	0.00339	0.09690	0.00725	0.00317	0.01063	0.00053	...	0.00004	0.11119	0.02555	0.05745	0.12331	0.02473	0.04735
p	0.13591	0.00018	0.00000	0.00000	0.18896	0.00000	0.00009	0.02051	0.05739	0.00000	...	0.00000	0.14626	0.02211	0.03802	0.03316	0.00000	0.00027
q	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	...	0.00000	0.00000	0.00000	0.00867	0.98844	0.00000	0.00000
r	0.06969	0.00347	0.01107	0.02439	0.23062	0.00331	0.00976	0.00205	0.09074	0.00003	...	0.00016	0.01756	0.05605	0.03938	0.01494	0.00534	0.00168
s	0.04452	0.00402	0.01574	0.00033	0.09858	0.00208	0.00052	0.06748	0.05475	0.00007	...	0.00033	0.00074	0.05058	0.12343	0.02614	0.00004	0.00538
t	0.04020	0.00032	0.01113	0.00016	0.08775	0.00084	0.00005	0.29901	0.07827	0.00002	...	0.00000	0.02447	0.02773	0.02079	0.01901	0.00102	0.00479
u	0.03328	0.01742	0.03949	0.03023	0.03322	0.00488	0.05552	0.00006	0.02158	0.00000	...	0.00006	0.11676	0.13317	0.16307	0.00000	0.00233	0.00022
v	0.07150	0.00000	0.00000	0.00025	0.57438	0.00000	0.00038	0.00000	0.23638	0.00000	...	0.00000	0.04488	0.00162	0.00000	0.00175	0.00000	0.00012
w	0.20861	0.00007	0.00021	0.00229	0.13725	0.00368	0.00007	0.19024	0.17290	0.00007	...	0.00000	0.00929	0.01345	0.00069	0.00028	0.00000	0.00160
x	0.17748	0.00000	0.10192	0.00000	0.15609	0.00071	0.00000	0.00784	0.08909	0.00000	...	0.01069	0.00000	0.00143	0.09979	0.03136	0.00000	0.00000
y	0.01323	0.00155	0.00163	0.00096	0.06873	0.00118	0.00007	0.00037	0.02062	0.00000	...	0.00000	0.00207	0.05025	0.01921	0.00022	0.00022	0.00377
z	0.11700	0.00221	0.00000	0.00221	0.46799	0.00000	0.00000	0.03974	0.18764	0.00000	...	0.00000	0.00000	0.00883	0.00000	0.03532	0.00221	0.00221

Figure: Probability of transitions for 150000 words text.

alphabets	a	b	c	d	e	f	g	h	i	j	...	q	r	s	t	u	v	w
a	0.00012	0.02157	0.03243	0.05554	0.00041	0.00698	0.01586	0.00197	0.04453	0.00028	...	0.00004	0.08345	0.09780	0.13720	0.00968	0.02020	0
b	0.07954	0.00490	0.00000	0.00102	0.33711	0.00000	0.00000	0.00013	0.03109	0.00903	...	0.00000	0.06434	0.02085	0.00928	0.15571	0.00439	0
c	0.12239	0.00000	0.01296	0.00011	0.17904	0.00000	0.00004	0.18857	0.06116	0.00000	...	0.00236	0.03198	0.00347	0.07689	0.03161	0.00000	0
d	0.02481	0.00086	0.00008	0.01011	0.10667	0.00084	0.00331	0.00188	0.07358	0.00023	...	0.00010	0.03371	0.02324	0.00067	0.01160	0.00207	0
e	0.04331	0.00119	0.01980	0.07385	0.02687	0.00886	0.00659	0.00207	0.01051	0.00029	...	0.00144	0.13793	0.06923	0.02668	0.00076	0.02760	0
f	0.07318	0.00017	0.00056	0.00069	0.10848	0.04803	0.00017	0.00004	0.07095	0.00009	...	0.00000	0.07082	0.00227	0.03359	0.04194	0.00000	0
g	0.05625	0.00021	0.00013	0.00030	0.10962	0.00009	0.00816	0.12538	0.05187	0.00000	...	0.00000	0.05110	0.01816	0.00266	0.02065	0.00000	0
h	0.16625	0.00042	0.00011	0.00015	0.44842	0.00069	0.00000	0.00007	0.15359	0.00000	...	0.00000	0.00790	0.00344	0.02678	0.01167	0.00038	0
i	0.01792	0.00794	0.04453	0.04935	0.03261	0.02217	0.02404	0.00074	0.00022	0.00009	...	0.00027	0.02923	0.12243	0.14606	0.00044	0.02657	0
j	0.04625	0.00000	0.00000	0.00000	0.25717	0.00000	0.00000	0.00000	0.00463	0.00000	...	0.00000	0.00000	0.00000	0.00000	0.45606	0.00000	0
k	0.08826	0.00041	0.00020	0.00000	0.24906	0.00041	0.00061	0.00061	0.17508	0.00000	...	0.00000	0.00255	0.02336	0.00051	0.00173	0.00010	0
l	0.07214	0.00111	0.00058	0.06654	0.18467	0.02520	0.00071	0.00027	0.11557	0.00000	...	0.00000	0.00330	0.01460	0.02474	0.01687	0.00477	0
m	0.14423	0.01553	0.00031	0.00000	0.25814	0.00222	0.00000	0.00019	0.09974	0.00000	...	0.00000	0.00093	0.03426	0.00051	0.03414	0.00000	0
n	0.02413	0.00042	0.03771	0.17551	0.07533	0.00512	0.14294	0.00106	0.02888	0.00095	...	0.00095	0.00032	0.04479	0.09668	0.00507	0.00467	0
o	0.00564	0.00667	0.00957	0.01456	0.00305	0.09244	0.00557	0.00291	0.01122	0.00033	...	0.00012	0.10599	0.02560	0.05901	0.12896	0.03099	0
p	0.12857	0.00049	0.00000	0.00005	0.19038	0.00000	0.00005	0.01824	0.05830	0.00000	...	0.00000	0.14242	0.02165	0.03736	0.03632	0.00000	0
q	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	...	0.00000	0.00000	0.00000	0.00548	0.99269	0.00000	0
r	0.06267	0.00324	0.01081	0.02467	0.22856	0.00359	0.01096	0.00198	0.08621	0.00005	...	0.00012	0.01951	0.05447	0.03859	0.01577	0.00569	0
s	0.05228	0.00440	0.01406	0.00029	0.10186	0.00228	0.00049	0.07013	0.05519	0.00007	...	0.00039	0.00048	0.05097	0.11827	0.02494	0.00103	0
t	0.03670	0.00023	0.01360	0.00011	0.08361	0.00090	0.00004	0.30155	0.07285	0.00001	...	0.00000	0.02383	0.02713	0.02183	0.01633	0.00082	0
u	0.02600	0.01746	0.03698	0.02576	0.03237	0.00464	0.05956	0.00122	0.02251	0.00000	...	0.00007	0.11356	0.13149	0.17132	0.00000	0.00241	0
v	0.07130	0.00000	0.00000	0.00015	0.54946	0.00000	0.00044	0.00000	0.25866	0.00000	...	0.00000	0.03798	0.00525	0.00095	0.00117	0.00000	0
w	0.21452	0.00016	0.00020	0.00199	0.13219	0.00342	0.00004	0.18672	0.17097	0.00004	...	0.00000	0.01110	0.01289	0.00044	0.00032	0.00000	0
x	0.26040	0.00000	0.08051	0.00000	0.21456	0.00039	0.00000	0.00539	0.06626	0.00000	...	0.00924	0.00000	0.00077	0.07935	0.01810	0.00000	0
y	0.01664	0.00137	0.00163	0.00084	0.07174	0.00110	0.00018	0.00044	0.02181	0.00000	...	0.00000	0.00207	0.04521	0.02159	0.00013	0.00071	0
z	0.11908	0.00135	0.00000	0.00135	0.38160	0.00000	0.00000	0.15968	0.15562	0.00000	...	0.00000	0.00000	0.00541	0.00000	0.02977	0.00135	0

Figure: Probability of transitions for 250000 words text.

for a random text the following results have been shown:



```
Unencrypted text:
  wake up to reality, nothing ever goes as planned in this accursed world. The longer you live, the more you will realize th
at the only thing that truly exist in this reality are merely suffering, pain and fertility futility. Everywhere you look in
this world, wherever there is light, there is always shadows to be found as well. As long as there is a concept of victors,
the vanquished will also exist. The selfish intent, of wanting to preserve peac, initite wars, and hatred is born in order t
o protect love. There are nexesus causal relationships that cannot be seperated. I want to sever the fate of this world,a  w
orld with only peace, a world with only victors, a world of only love.

Encrypted text:
  HXMI QS LO FIXPTLJ  ZOLNTZU IWIF UOIY XY SPXZZID TZ LNTY XVVQFYID HOFPD  LNI POZUIF JOQ PTWI  LNI GOFI JOQ HTPP FIXPTEI LN
XL LNI OZPJ LNTZU LNXL LFQPJ IATYL TZ LNTY FIXPTLJ XFI GIFIPJ YQRRIFTZU  SXTZ XZD RIFLTPTLJ RQLTPTLJ  IWIFJHNIFI JOQ POOM TZ
LNTY HOFPD  HNIFIWIF LNIFI TY PTUNL  LNIFI TY XPHXJY YNXDOHY LO BI ROQZD XY HIPP
```

Figure: Before and after encryption.

```
Iter: 0  WAKE UP NO REALIND  TONGITH EVER HOES AS PLATTEY IT NGIS AFFURSEY WORLY  NGE LOTHER DOU LI
VE  NGE
Iter: 500  WAVE UP NO REALIND  TONGITH EMER HOES AS PLATTEY IT NGIS AFFURSEY WORLY  NGE LOTHER DOU
LIME  NGE
Iter: 1000  WAKE UF NO REALIND  TONGITH EVER HOES AS FLATTEY IT NGIS APPURSEY WORLY  NGE LOTHER DOU
LIVE  NGE
Iter: 1500  WABE UP NO REALIND  TONGITH EMER HOES AS PLATTEY IT NGIS AFFURSEY WORLY  NGE LOTHER DOU
LIME  NGE
Iter: 2000  WAKE UM NO REALIND  TONGITH EVER HOES AS MLATTEY IT NGIS AFFURSEY WORLY  NGE LOTHER DOU
LIVE  NGE
Iter: 2500  WAKE UP NO REALIND  TONGITH EVER HOES AS PLATTEY IT NGIS AFFURSEY WORLY  NGE LOTHER DOU
LIVE  NGE
Iter: 3000  WAKE UP NO REALIND  TONGITH EVER HOES AS PLATTEY IT NGIS ACCURSEY WORLY  NGE LOTHER DOU
LIVE  NGE
Iter: 3500  WAFE UP NO REALIND  TONGITH EVER HOES AS PLATTEY IT NGIS ABBURSEY WORLY  NGE LOTHER DOU
LIVE  NGE
Iter: 4000  WAKE UP NO REALIND  TONGITH EVER HOES AS PLATTEY IT NGIS AFFURSEY WORLY  NGE LOTHER DOU
LIVE  NGE
```

Figure: first few hundreds of iterations

```
Iter: 18000  WAME UP NO REALIND  TONGITH EVER HOES AS PLATTEY IT NGIS AFFURSEY WORLY  NGE LOTHER DO
U LIVE  NGE
Iter: 18500  WAKE UC NO REALIND  TONGITH EVER HOES AS CLATTEY IT NGIS AFFURSEY WORLY  NGE LOTHER DO
U LIVE  NGE
Iter: 19000  WAME UP NO REALIND  TONGITH EVER HOES AS PLATTEY IT NGIS AFFURSEY WORLY  NGE LOTHER DO
U LIVE  NGE
Iter: 19500  WAME UP NO REALIND  TONGITH EVER HOES AS PLATTEY IT NGIS AFFURSEY WORLY  NGE LOTHER DO
U LIVE  NGE
Iter: 20000  WAME UP NO REALIND  TONGITH EVER HOES AS PLATTEY IT NGIS AFFURSEY WORLY  NGE LOTHER DO
U LIVE  NGE

Decrypted text:
 WAME UP NO REALIND  TONGITH EVER HOES AS PLATTEY IT NGIS AFFURSEY WORLY  NGE LOTHER DOU LIVE  NGE
BORE DOU WILL REALIKE NGAN NGE OTLD NGITH NGAN NRULD EXISN IT NGIS REALIND ARE BERELD SUCCERITH  PA
IT ATY CERNILIND CUNILIND  EVERDWGERE DOU LOOM IT NGIS WORLY  WGEREVER NGERE IS LIHGN  NGERE IS ALW
ADS SGAYOWS NO JE COUTY AS WELL


Number of correctly decoded letters: 12
```

Figure: last few hundreds of iterations.

Graphing

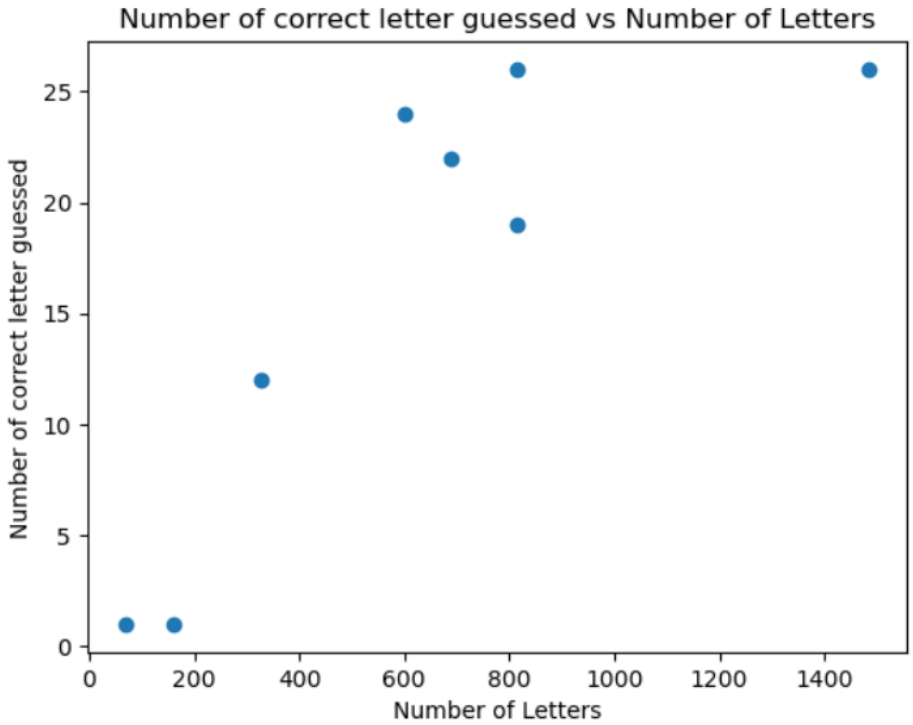


Figure: Scatter plot of correctly guessed letter vs number of letters used

Curve Fit

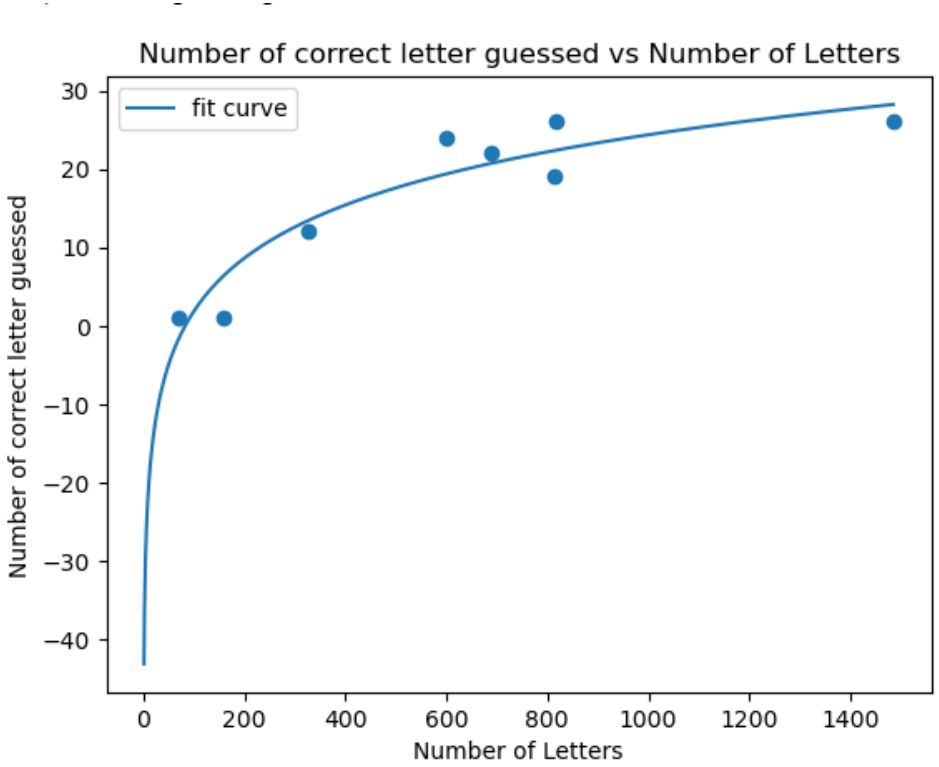


Figure: logarithmic Curve fit of our data

Conclusion

The results show that we need approximately 1183 encrypted words to get the 26 letters correctly guessed