Homework 2 CMPS 122

John Carlyle

February 5, 2014

1. Problem one took the longest by far. I started by reading decrypt and encrypt and trying to clone the decrypt.c file in a repeat loop. My code had frusteratingly close to realistic looking results for a few days until I realized I had placed indicies 0 1 2 4 for copying bits into a char array. Which is wrong. Check the aes directory in the compressed attachment.

   ```
   make all ; ./jcdecrypt hw2.txt.crypt
   ```

   The program will brute force for a little while and print out all candidate keys. If some key decrypts the ciphertext and reveals something that looks like ascii the program alerts the uesr by showing the little snippit of plaintext and the password used to generate that. Once I saw the obvious plaintext go by (THE PURLOINED LE), I stoped the program and copied the password which is: 9E412AD800000000000000000000000. The plaintext wasn't the first one too look like ascii, so I could see this approach having more trouble if the keyspace were larger, well that and the obvious downside of a large keyspace.

   ```
   ./decrypt 9E412AD800000000000000000000000 cbc hw2.txt.crypt
   ```

   reveals the hidden message. The message is attached to the end of this PDF as requested in the prompt.

2. The s-box cannot be a linear transform otherwise it introduces the vulnerabilities displayed in the last part of the previous homework. Any substitution would technically work though, it just may not be secure.

3. A hash function could be used as part of an encryption algorithm if it were used as the substitution function. Some constraints would have to be put on the hashing function given the set of values we needed for the table. For example it would probably not be good if there was a collision. Having a hashing function as an s-box would be probably be useful given that a hashing function is non-linear.

4. $RSAH(b_1, b_2) := RSA(RSA(b_1) \oplus b_2)$

   $RSAH(c_1, c_2) = RSAH(b_1, b_2)$
   $RSA(RSA(c_1) \oplus c_2) = RSA(RSA(b_1) \oplus b_2)$
   Since we know the key to RSA
   $RSA(c_1) \oplus c_2 = RSA(b_1) \oplus b_2$
   Handily enough xor is its own inverse!
   $c_2 = RSA(b_1) \oplus b_2 \oplus RSA(c_1)$

   And there you have a simple way to choose c_1 in such a way as to get a collision.

5. RSA encryption should be secure against a chosen plaintext attack. Meaning even if the person knows what the text is and the public key, they still cannot recover the private key this should be obvious since everyone has access to the public key and can generate however many chosen texts they want. I say should because it can be implemented terribly and the numbers chosen can be artificially small making it easier to calculate the secret keys. RSA also should supply enough diffusion that the pattern should not be spotted assuming the attacker only has access to the ciphertext. Since the message is a number that is being exponentiated repeatedly.

6.

Check the files realSha.py and fakeSha.py for the generation of these messages. It took about 11 seconds total on my computer. There were quite a few collisions to choose from, I tried to pick a pair with the minimum number of random capitalization changes. Eighteen nested repeat loops, easily my best work. The code can be executed as such:

```
python realSha.py ; python fakeSha.py
```

The first command generates all the real messagse and their hashes and saves them to a file. The second command reads the file and then starts computing hashes of fake messages looking for a hash that was already created by the previous process. Whenever a match is found it prints both messages and their shared hash.

Message for the Judge I James Smith authorize the sale of 1800 West Cliff dr. in S.C. to John William Carlyle for 1 Million dollars on Feb. 6 2014

Message for the Seller I mr smith authorize the sale of 1800 West cliff Dr. in Santa Cruz to J. W. Carlyle for $1.5 million on Feb. 4 2014

Both hash (last 10 hex) to: 7b2f570947

THE PURLOINED LETTER

by Edgar Allan Poe (1845) Nil sapientiae odiosius acumine nimio. - Seneca.

At Paris, just after dark one gusty evening in the autumn of 18–, I was enjoying the twofold luxury of meditation and a meerschaum, in company with my friend C. Auguste Dupin, in his little back library, or book-closet, au troisieme, No. 33, Rue Dunot, Faubourg St. Germain. For one hour at least we had maintained a profound silence; while each, to any casual observer, might have seemed intently and exclusively occupied with the curling eddies of smoke that oppressed the atmosphere of the chamber. For myself, however, I was mentally discussing certain topics which had formed matter for conversation between us at an earlier period of the evening; I mean the affair of the Rue Morgue, and the mystery attending the murder of Marie Roget. I looked upon it, therefore, as something of a coincidence, when the door of our apartment was thrown open and admitted our old acquaintance, Monsieur G–, the Prefect of the Parisian police.

We gave him a hearty welcome; for there was nearly half as much of the entertaining as of the contemptible about the man, and we had not seen him for several years. We had been sitting in the dark, and Dupin now arose for the purpose of lighting a lamp, but sat down again, without doing so, upon G.'s saying that he had called to consult us, or rather to ask the opinion of my friend, about some official business which had occasioned a great deal of trouble.

"If it is any point requiring reflection," observed Dupin, as he forbore to enkindle the wick, "we shall examine it to better purpose in the dark."

"That is another of your odd notions," said the Prefect, who had a fashion of calling every thing "odd" that was beyond his comprehension, and thus lived amid an absolute legion of "oddities."

"Very true," said Dupin, as he supplied his visitor with a pipe, and rolled towards him a comfortable chair.

"And what is the difficulty now?" I asked. "Nothing more in the assassination way, I hope?"

"Oh no; nothing of that nature. The fact is, the business is very simple indeed, and I make no doubt that we can manage it sufficiently well ourselves; but then I thought Dupin would like to hear the details of it, because it is so excessively odd."

"Simple and odd," said Dupin.

"Why, yes; and not exactly that, either. The fact is, we have all been a good deal puzzled because the affair is so simple, and yet baffles us altogether."

"Perhaps it is the very simplicity of the thing which puts you at fault," said my friend.

"What nonsense you do talk!" replied the Prefect, laughing heartily.

"Perhaps the mystery is a little too plain," said Dupin.

"Oh, good heavens! who ever heard of such an idea?"

"A little too self-evident."

"Ha! ha! ha! –ha! ha! ha! –ho! ho! ho!" –roared our visitor, profoundly amused, "oh, Dupin, you will be the death of me yet!"

"And what, after all, is the matter on hand?" I asked.

"Why, I will tell you," replied the Prefect, as he gave a long, steady, and contemplative puff, and settled himself in his chair. "I will tell you in a few words; but, before I begin, let me caution you that this is an affair demanding the greatest secrecy, and that I should most probably lose the position I now hold, were it known that I confided it to any one.

"Proceed," said I.

"Or not," said Dupin.

"Well, then; I have received personal information, from a very high quarter, that a certain document of the last importance, has been purloined from the royal apartments. The individual who purloined it is known; this beyond a doubt; he was seen to take it. It is known, also, that it still remains in his possession."

"How is this known?" asked Dupin.

"It is clearly inferred," replied the Prefect, "from the nature of the document, and from the nonappearance of certain results which would at once arise from its passing out of the robber's possession; –that is to say, from his employing it as he must design in the end to employ it."

"Be a little more explicit," I said.

"Well, I may venture so far as to say that the paper gives its holder a certain power in a certain quarter where such power is immensely valuable." The Prefect was fond of the cant of diplomacy.

"Still I do not quite understand," said Dupin.

"No? Well; the disclosure of the document to a third person, who shall be nameless, would bring in question the honor of a personage of most exalted station; and this fact gives the holder of the document an ascendancy over the illustrious personage whose honor and peace are so jeopardized."

"But this ascendancy," I interposed, "would depend upon the robber's knowledge of the loser's knowledge of the robber. Who would dare–"

"The thief," said G., is the Minister D–, who dares all things, those unbecoming as well as those becoming a man. The method of the theft was not less ingenious than bold. The document in question –a letter, to be frank –had been received by the personage robbed while alone in the royal boudoir. During its perusal she was suddenly interrupted by the entrance of the other exalted personage from whom especially it was her wish to conceal it. After a hurried and vain endeavor to thrust it in a drawer, she was forced to place it, open as it was, upon a table. The address, however, was uppermost, and, the contents thus unexposed, the letter escaped notice. At this juncture enters the Minister D–. His lynx eye immediately perceives the paper, recognises the handwriting of the address, observes the confusion of the personage addressed, and fathoms her secret. After some business transactions, hurried through in his ordinary manner, he produces a letter somewhat similar to the one in question, opens it, pretends to read it, and then places it in close juxtaposition to the other. Again he converses, for some fifteen minutes, upon the public affairs. At length, in taking leave, he takes also from the table the letter to which he had no claim. Its rightful owner saw, but, of course, dared not call attention to the act, in the presence of the third personage who stood at her elbow. The minister decamped; leaving his own letter –one of no importance –upon the table."

"Here, then," said Dupin to me, "you have precisely what you demand to make the ascendancy complete –the robber's knowledge of the loser's knowledge of the robber."

"Yes," replied the Prefect; "and the power thus attained has, for some months past, been wielded, for political purposes, to a very dangerous extent. The personage robbed is more thoroughly convinced, every day, of the necessity of reclaiming her letter. But this, of course, cannot be done openly. In fine, driven to despair, she has committed the matter to me."

"Than whom," said Dupin, amid a perfect whirlwind of smoke, "no more sagacious agent could, I suppose, be desired, or even imagined."

"You flatter me," replied the Prefect; "but it is possible that some such opinion may have been entertained."

"It is clear," said I, "as you observe, that the letter is still in possession of the minister; since it is this possession, and not any employment of the letter, which bestows the power. With the employment the power departs."

"True," said G. "and upon this conviction I proceeded. My first care was to make thorough search of the minister's hotel; and here my chief embarrassment lay in the necessity of searching without his knowledge. Beyond all things, I have been warned of the danger which would result from giving him reason to suspect our design."

"But," said I, "you are quite au fait in these investigations. The Parisian police have done this thing often before."

"Oh yes; and for this reason I did not despair. The habits of the minister gave me, too, a great advantage. He is frequently absent from home all night. His servants are by no means numerous. They sleep at a distance from their master's apartment, and, being chiefly Neapolitans, are readily made drunk. I have keys, as you know, with

which I can open any chamber or cabinet in Paris. For three months a night has not passed, during the greater part of which I have not been engaged, personally, in ransacking the D– Hotel. My honor is interested, and, to mention a great secret, the reward is enormous. So I did not abandon the search until I had become fully satisfied that the thief is a more astute man than myself. I fancy that I have investigated every nook and corner of the premises in which it is possible that the paper can be concealed."

"But is it not possible," I suggested, "that although the letter may be in possession of the minister, as it unquestionably is, he may have concealed it elsewhere than upon his own premises?"

"This is barely possible," said Dupin. "The present peculiar condition of affairs at court, and especially of those intrigues in which D– is known to be involved, would render the instant availability of the document –its susceptibility of being produced at a moment's notice –a point of nearly equal importance with its possession."

"Its susceptibility of being produced?" said I.

"That is to say, of being destroyed," said Dupin.

"True," I observed; "the paper is clearly then upon the premises. As for its being upon the person of the minister, we may consider that as out of the question."

"Entirely," said the Prefect. "He has been twice waylaid, as if by footpads, and his person rigorously searched under my own inspection.

"You might have spared yourself this trouble," said Dupin. "D–, I presume, is not altogether a fool, and, if not, must have anticipated these waylayings, as a matter of course."

"Not altogether a fool," said G., "but then he's a poet, which I take to be only one remove from a fool."

"True," said Dupin, after a long and thoughtful whiff from his meerschaum, "although I have been guilty of certain doggerel myself."

"Suppose you detail," said I, "the particulars of your search."

"Why the fact is, we took our time, and we searched every where. I have had long experience in these affairs. I took the entire building, room by room; devoting the nights of a whole week to each. We examined, first, the furniture of each apartment. We opened every possible drawer; and I presume you know that, to a properly trained police agent, such a thing as a secret drawer is impossible. Any man is a dolt who permits a 'secret' drawer to escape him in a search of this kind. The thing is so plain. There is a certain amount of bulk –of space –to be accounted for in every cabinet. Then we have accurate rules. The fiftieth part of a line could not escape us. After the cabinets we took the chairs. The cushions we probed with the fine long needles you have seen me employ. From the tables we removed the tops."

"Why so?"

"Sometimes the top of a table, or other similarly arranged piece of furniture, is removed by the person wishing to conceal an article; then the leg is excavated, the article deposited within the cavity, and the top replaced. The bottoms and tops of bedposts are employed in the same way."

"But could not the cavity be detected by sounding?" I asked.

"By no means, if, when the article is deposited, a sufficient wadding of cotton be placed around it. Besides, in our case, we were obliged to proceed without noise."

"But you could not have removed –you could not have taken to pieces all articles of furniture in which it would have been possible to make a deposit in the manner you mention. A letter may be compressed into a thin spiral roll, not differing much in shape or bulk from a large knitting-needle, and in this form it might be inserted into the rung of a chair, for example. You did not take to pieces all the chairs?"

"Certainly not; but we did better –we examined the rungs of every chair in the hotel, and, indeed, the jointings of every description of furniture, by the aid of a most powerful microscope. Had there been any traces of recent disturbance we should not have failed to detect it instantly. A single grain of gimlet-dust, for example, would have been as obvious as an apple. Any disorder in the glueing –any unusual gaping in the joints –would have sufficed to insure detection."

"I presume you looked to the mirrors, between the boards and the plates, and you probed the beds and the bed-clothes, as well as the curtains and carpets."

"That of course; and when we had absolutely completed every particle of the furniture in this way, then we examined the house itself. We divided its entire surface into compartments, which we numbered, so that none might be missed; then we scrutinized each individual square inch throughout the premises, including the two houses immediately adjoining, with the microscope, as before."

"The two houses adjoining!" I exclaimed; "you must have had a great deal of trouble."

"We had; but the reward offered is prodigious.

"You include the grounds about the houses?"

"All the grounds are paved with brick. They gave us comparatively little trouble. We examined the moss between the bricks, and found it undisturbed."

"You looked among D–'s papers, of course, and into the books of the library?"

"Certainly; we opened every package and parcel; we not only opened every book, but we turned over every leaf in each volume, not contenting ourselves with a mere shake, according to the fashion of some of our police officers. We also measured the thickness of every book-cover, with the most accurate admeasurement, and applied to each the most jealous scrutiny of the microscope. Had any of the bindings been recently meddled with, it would have been utterly impossible that the fact should have escaped observation. Some five or six volumes, just from the hands of the binder, we carefully probed, longitudinally, with the needles."

"You explored the floors beneath the carpets?"

"Beyond doubt. We removed every carpet, and examined the boards with the microscope."

"And the paper on the walls?"

"Yes.

"You looked into the cellars?"

"We did."

"Then," I said, "you have been making a miscalculation, and the letter is not upon the premises, as you suppose.

"I fear you are right there," said the Prefect. "And now, Dupin, what would you advise me to do?"

"To make a thorough re-search of the premises."

"That is absolutely needless," replied G–. "I am not more sure that I breathe than I am that the letter is not at the Hotel."

"I have no better advice to give you," said Dupin. "You have, of course, an accurate description of the letter?"

"Oh yes!" –And here the Prefect, producing a memorandum-book, proceeded to read aloud a minute account of the internal, and especially of the external appearance of the missing document. Soon after finishing the perusal of this description, he took his departure, more entirely depressed in spirits than I had ever known the good gentleman before.

In about a month afterwards he paid us another visit, and found us occupied very nearly as before. He took a pipe and a chair and entered into some ordinary conversation. At length I said,–

"Well, but G–, what of the purloined letter? I presume you have at last made up your mind that there is no such thing as overreaching the Minister?"

"Confound him, say I –yes; I made the reexamination, however, as Dupin suggested –but it was all labor lost, as I knew it would be."

"How much was the reward offered, did you say?" asked Dupin.

"Why, a very great deal –a very liberal reward –I don't like to say how much, precisely; but one thing I will say, that I wouldn't mind giving my individual check for fifty thousand francs to any one who could obtain me that

letter. The fact is, it is becoming of more and more importance every day; and the reward has been lately doubled. If it were trebled, however, I could do no more than I have done."

"Why, yes," said Dupin, drawlingly, between the whiffs of his meerschaum, "I really –think, G–, you have not exerted yourself–to the utmost in this matter. You might –do a little more, I think, eh?"

"How? –In what way?"

"Why –puff, puff –you might –puff, puff –employ counsel in the matter, eh? –puff, puff, puff. Do you remember the story they tell of Abernethy?"

"No; hang Abernethy!"

"To be sure! hang him and welcome. But, once upon a time, a certain rich miser conceived the design of spunging upon this Abernethy for a medical opinion. Getting up, for this purpose, an ordinary conversation in a private company, he insinuated his case to the physician, as that of an imaginary individual.

"'We will suppose,' said the miser, 'that his symptoms are such and such; now, doctor, what would you have directed him to take?'

"'Take!' said Abernethy, 'why, take advice, to be sure.'"

"But," said the Prefect, a little discomposed, "I am perfectly willing to take advice, and to pay for it. I would really give fifty thousand francs to any one who would aid me in the matter."

"In that case," replied Dupin, opening a drawer, and producing a check-book, "you may as well fill me up a check for the amount mentioned. When you have signed it, I will hand you the letter."

I was astounded. The Prefect appeared absolutely thunderstricken. For some minutes he remained speechless and motionless, less, looking incredulously at my friend with open mouth, and eyes that seemed starting from their sockets; then, apparently in some measure, he seized a pen, and after several pauses and vacant stares, finally filled up and signed a check for fifty thousand francs, and handed it across the table to Dupin. The latter examined it carefully and deposited it in his pocket-book; then, unlocking an escritoire, took thence a letter and gave it to the Prefect. This functionary grasped it in a perfect agony of joy, opened it with a trembling hand, cast a rapid glance at its contents, and then, scrambling and struggling to the door, rushed at length unceremoniously from the room and from the house, without having uttered a syllable since Dupin had requested him to fill up the check.

When he had gone, my friend entered into some explanations.

"The Parisian police," he said, "are exceedingly able in their way. They are persevering, ingenious, cunning, and thoroughly versed in the knowledge which their duties seem chiefly to demand. Thus, when G– detailed to us his mode of searching the premises at the Hotel D–, I felt entire confidence in his having made a satisfactory investigation –so far as his labors extended."

"So far as his labors extended?" said I.

"Yes," said Dupin. "The measures adopted were not only the best of their kind, but carried out to absolute perfection. Had the letter been deposited within the range of their search, these fellows would, beyond a question, have found it."

I merely laughed –but he seemed quite serious in all that he said.

"The measures, then," he continued, "were good in their kind, and well executed; their defect lay in their being inapplicable to the case, and to the man. A certain set of highly ingenious resources are, with the Prefect, a sort of Procrustean bed, to which he forcibly adapts his designs. But he perpetually errs by being too deep or too shallow, for the matter in hand; and many a schoolboy is a better reasoner than he. I knew one about eight years of age, whose success at guessing in the game of 'even and odd' attracted universal admiration. This game is simple, and is played with marbles. One player holds in his hand a number of these toys, and demands of another whether that number is even or odd. If the guess is right, the guesser wins one; if wrong, he loses one. The boy to whom I allude won all the marbles of the school. Of course he had some principle of guessing; and this lay in mere observation and admeasurement of the astuteness of his opponents. For example, an arrant simpleton is his opponent, and, holding up his closed hand, asks, 'are they even or odd?' Our schoolboy replies, 'odd,' and loses; but upon the second trial he wins, for he then says to himself, the simpleton had them even upon the first trial, and his amount of cunning is just sufficient to make him have them odd upon the second; I will therefore guess odd'; –he guesses odd, and wins. Now, with a simpleton a degree above the first, he would have reasoned thus: 'This fellow finds that in the first instance I guessed odd, and, in the second, he will propose to himself upon the first impulse, a simple variation from even to odd, as did the first simpleton; but then a second thought will suggest that this is too simple a variation, and finally he will decide upon putting it even as before. I will therefore guess even' guesses even, and wins. Now this mode of reasoning in the schoolboy, whom his fellows termed "lucky," –what, in its last analysis, is it?"

"It is merely," I said, "an identification of the reasoner's intellect with that of his opponent."

"It is," said Dupin;" and, upon inquiring of the boy by what means he effected the thorough identification in which his success consisted, I received answer as follows: 'When I wish to find out how wise, or how stupid, or how good, or how wicked is any one, or what are his thoughts at the moment, I fashion the expression of my face, as accurately as possible, in accordance with the expression of his, and then wait to see what thoughts or sentiments arise in my mind or heart, as if to match or correspond with the expression.' This response of the schoolboy lies at the bottom of all the spurious profundity which has been attributed to Rochefoucauld, to La Bougive, to Machiavelli, and to Campanella."

"And the identification," I said, "of the reasoner's intellect with that of his opponent, depends, if I understand you aright upon the accuracy with which the opponent's intellect is admeasured."

"For its practical value it depends upon this," replied Dupin; and the Prefect and his cohort fall so frequently, first, by default of this identification, and, secondly, by ill-admeasurement, or rather through non-admeasurement, of the intellect with which they are engaged. They consider only their own ideas of ingenuity; and, in searching for anything hidden, advert only to the modes in which they would have hidden it. They are right in this much –that their own ingenuity is a faithful representative of that of the mass; but when the cunning of the individual felon is diverse in character from their own, the felon foils them, of course. This always happens when it is above their own, and very usually when it is below. They have no variation of principle in their investigations; at best, when urged by some unusual emergency –by some extraordinary reward –they extend or exaggerate their old modes of practice, without touching their principles. What, for example, in this case of D–, has been done to vary the principle of action? What is all this boring, and probing, and sounding, and scrutinizing with the microscope, and dividing the surface of the building into registered square inches –what is it all but an exaggeration of the application of the one principle or set of principles of search, which are based upon the one set of notions regarding human ingenuity, to which the Prefect, in the long routine of his duty, has been accustomed? Do you not see he has taken it for granted that all men proceed to conceal a letter, –not exactly in a gimlet-hole bored in a chair-leg –but, at least, in some hole or corner suggested by the same tenor of thought which would urge a man to secrete a letter in a gimlet-hole bored in a chair-leg? And do you not see also, that such recherches nooks for concealment are adapted only for ordinary occasions, and would be adopted only by ordinary intellects; for, in all cases of concealment, a disposal of the article concealed –a disposal of it in this recherche manner, –is, in the very first instance, presumable and presumed; and thus its discovery depends, not at all upon the acumen, but altogether upon the mere care, patience, and determination of the seekers; and where the case is of importance –or, what amounts to the same thing in the policial eyes, when the reward is of magnitude, –the qualities in question have never been known to fall. You will now understand what I meant in suggesting that, had the purloined letter been hidden anywhere within the limits of the Prefect's examination –in other words, had the principle of its concealment been comprehended within the principles of the Prefect –its discovery would have been a matter altogether beyond question. This functionary, however, has been thoroughly mystified; and the remote source of his defeat lies in the supposition that the Minister is a fool, because he has acquired renown as a poet. All fools are poets; this the Prefect feels; and he is merely guilty of a non distributio medii in thence inferring that all poets are fools."

"But is this really the poet?" I asked. "There are two brothers, I know; and both have attained reputation in letters. The Minister I believe has written learnedly on the Differential Calculus. He is a mathematician, and no poet."

"You are mistaken; I know him well; he is both. As poet and mathematician, he would reason well; as mere mathematician, he could not have reasoned at all, and thus would have been at the mercy of the Prefect."

"You surprise me," I said, "by these opinions, which have been contradicted by the voice of the world. You do not mean to set at naught the well-digested idea of centuries. The mathematical reason has long been regarded as the reason par excellence.

"'Il y a a parier,'" replied Dupin, quoting from Chamfort, "'que toute idee publique, toute convention recue, est une sottise, car elle a convenu au plus grand nombre.' The mathematicians, I grant you, have done their best to promulgate the popular error to which you allude, and which is none the less an error for its promulgation as truth. With an art worthy a better cause, for example, they have insinuated the term 'analysis' into application to algebra. The French are the originators of this particular deception; but if a term is of any importance –if words derive any value from applicability –then 'analysis' conveys 'algebra' about as much as, in Latin, 'ambitus' implies 'ambition,' 'religio' religion or 'homines honesti,' a set of honorable men."

"You have a quarrel on hand, I see," said I, "with some of the algebraists of Paris; but proceed."

"I dispute the availability, and thus the value, of that reason which is cultivated in any especial form other than the abstractly logical. I dispute, in particular, the reason educed by mathematical study. The mathematics are the science of form and quantity; mathematical reasoning is merely logic applied to observation upon form and quantity. The great error lies in supposing that even the truths of what is called pure algebra, are abstract or general truths. And this error is so egregious that I am confounded at the universality with which it has been received. Mathematical axioms are not axioms of general truth. What is true of relation –of form and quantity –is often grossly false in regard to morals, for example. In this latter science it is very usually untrue that the aggregated parts are equal to the whole. In chemistry also the axiom falls. In the consideration of motive it falls; for two motives, each of a given value, have not, necessarily, a value when united, equal to the sum of their values apart. There are numerous other mathematical truths which are only truths within the limits of relation. But the mathematician argues, from his finite truths, through habit, as if they were of an absolutely general applicability –as the world indeed imagines them to be. Bryant, in his very learned 'Mythology,' mentions an analogous source of error, when he says that 'although the Pagan fables are not believed, yet we forget ourselves continually, and make inferences from them as existing realities.' With the algebraists, however, who are Pagans themselves, the 'Pagan fables' are believed, and the inferences are made, not so much through lapse of memory, as through an unaccountable addling of the brains. In short, I never yet encountered the mere mathematician who could be trusted out of equal roots, or one who did not clandestinely hold it as a point of his faith that x squared + px was absolutely and unconditionally equal to q. Say to one of these gentlemen, by way of experiment, if you please, that you believe occasions may occur where x squared + px is not altogether equal to q, and, having made him understand what you mean, get out of his reach as speedily as convenient, for, beyond doubt, he will endeavor to knock you down.

I mean to say," continued Dupin, while I merely laughed at his last observations, "that if the Minister had been no more than a mathematician, the Prefect would have been under no necessity of giving me this check. I knew him, however, as both mathematician and poet, and my measures were adapted to his capacity, with reference to the circumstances by which he was surrounded. I knew him as a courtier, too, and as a bold intriguant. Such a man, I considered, could not fail to be aware of the ordinary policial modes of action. He could not have failed to anticipate –and events have proved that he did not fail to anticipate –the waylayings to which he was subjected. He must have foreseen, I reflected, the secret investigations of his premises. His frequent absences from home at night, which were hailed by the Prefect as certain aids to his success, I regarded only as ruses, to afford opportunity for thorough search to the police, and thus the sooner to impress them with the conviction to which G–, in fact, did finally arrive –the conviction that the letter was not upon the premises. I felt, also, that the whole train of thought, which I was at some pains in detailing to you just now, concerning the invariable principle of policial action in searches for articles concealed –I felt that this whole train of thought would necessarily pass through the mind of the Minister. It would imperatively lead him to despise all the ordinary nooks of concealment. He could not, I reflected, be so weak as not to see that the most intricate and remote recess of his hotel would be as open as his commonest closets to the eyes, to the probes, to the gimlets, and to the microscopes of the Prefect. I saw, in fine, that he would be driven, as a matter of course, to simplicity, if not deliberately induced to it as a matter of choice. You will remember, perhaps, how desperately the Prefect laughed when I suggested, upon our first interview, that it was just possible this mystery troubled him so much on account of its being so very self-evident."

"Yes," said I, "I remember his merriment well. I really thought he would have fallen into convulsions."

"The material world," continued Dupin, "abounds with very strict analogies to the immaterial; and thus some color of truth has been given to the rhetorical dogma, that metaphor, or simile, may be made to strengthen an argument, as well as to embellish a description. The principle of the vis inertiae, for example, seems to be identical in physics and metaphysics. It is not more true in the former, that a large body is with more difficulty set in motion than a smaller one, and that its subsequent momentum is commensurate with this difficulty, than it is, in the latter, that intellects of the vaster capacity, while more forcible, more constant, and more eventful in their movements than those of inferior grade, are yet the less readily moved, and more embarrassed and full of hesitation in the first few steps of their progress. Again: have you ever noticed which of the street signs, over the shop doors, are the most attractive of attention?"

"I have never given the matter a thought," I said.

"There is a game of puzzles," he resumed, "which is played upon a map. One party playing requires another to find a given word –the name of town, river, state or empire –any word, in short, upon the motley and perplexed surface of the chart. A novice in the game generally seeks to embarrass his opponents by giving them the most minutely lettered names; but the adept selects such words as stretch, in large characters, from one end of the chart to the other. These, like the over-largely lettered signs and placards of the street, escape observation by dint of being excessively obvious; and here the physical oversight is precisely analogous with the moral inapprehension by which the intellect suffers to pass unnoticed those considerations which are too obtrusively and too palpably self-evident. But this is a point, it appears, somewhat above or beneath the understanding of the Prefect. He never once thought it probable, or possible, that the Minister had deposited the letter immediately beneath the nose of the whole world, by way of best preventing any portion of that world from perceiving it.

"But the more I reflected upon the daring, dashing, and discriminating ingenuity of D–; upon the fact that the document must always have been at hand, if he intended to use it to good purpose; and upon the decisive evidence, obtained by the Prefect, that it was not hidden within the limits of that dignitary's ordinary search –the more satisfied I became that, to conceal this letter, the Minister had resorted to the comprehensive and sagacious expedient of not attempting to conceal it at all.

"Full of these ideas, I prepared myself with a pair of green spectacles, and called one fine morning, quite by accident, at the Ministerial hotel. I found D– at home, yawning, lounging, and dawdling, as usual, and pretending to be in the last extremity of ennui. He is, perhaps, the most really energetic human being now alive –but that is only when nobody sees him.

"To be even with him, I complained of my weak eyes, and lamented the necessity of the spectacles, under cover of which I cautiously and thoroughly surveyed the apartment, while seemingly intent only upon the conversation of my host.

"I paid special attention to a large writing-table near which he sat, and upon which lay confusedly, some miscellaneous letters and other papers, with one or two musical instruments and a few books. Here, however, after a long and very deliberate scrutiny, I saw nothing to excite particular suspicion.

"At length my eyes, in going the circuit of the room, fell upon a trumpery filigree card-rack of pasteboard, that hung dangling by a dirty blue ribbon, from a little brass knob just beneath the middle of the mantelpiece. In this rack, which had three or four compartments, were five or six visiting cards and a solitary letter. This last was much soiled and crumpled. It was torn nearly in two, across the middle –as if a design, in the first instance, to tear it entirely up as worthless, had been altered, or stayed, in the second. It had a large black seal, bearing the D– cipher very conspicuously, and was addressed, in a diminutive female hand, to D–, the minister, himself. It was thrust carelessly, and even, as it seemed, contemptuously, into one of the upper divisions of the rack.

"No sooner had I glanced at this letter, than I concluded it to be that of which I was in search. To be sure, it was, to all appearance, radically different from the one of which the Prefect had read us so minute a description. Here the seal was large and black, with the D– cipher; there it was small and red, with the ducal arms of the S– family. Here, the address, to the Minister, was diminutive and feminine; there the superscription, to a certain royal personage, was markedly bold and decided; the size alone formed a point of correspondence. But, then, the radicalness of these differences, which was excessive; the dirt; the soiled and torn condition of the paper, so inconsistent with the true methodical habits of D–, and so suggestive of a design to delude the beholder into an idea of the worthlessness of the document; these things, together with the hyperobtrusive situation of this document, full in the view of every visitor, and thus exactly in accordance with the conclusions to which I had previously arrived; these things, I say, were strongly corroborative of suspicion, in one who came with the intention to suspect.

"I protracted my visit as long as possible, and, while I maintained a most animated discussion with the Minister, on a topic which I knew well had never failed to interest and excite him, I kept my attention really riveted upon the letter. In this examination, I committed to memory its external appearance and arrangement in the rack; and also fell, at length, upon a discovery which set at rest whatever trivial doubt I might have entertained. In scrutinizing the edges of the paper, I observed them to be more chafed than seemed necessary. They presented the broken appearance which is manifested when a stiff paper, having been once folded and pressed with a folder, is refolded in a reversed direction, in the same creases or edges which had formed the original fold. This discovery was sufficient. It was clear to me that the letter had been turned, as a glove, inside out, re-directed, and re-sealed. I bade the Minister good morning, and took my departure at once, leaving a gold snuff-box upon the table.

"The next morning I called for the snuff-box, when we resumed, quite eagerly, the conversation of the preceding day. While thus engaged, however, a loud report, as if of a pistol, was heard immediately beneath the windows of the hotel, and was succeeded by a series of fearful screams, and the shoutings of a mob. D– rushed to a casement, threw it open, and looked out. In the meantime, I stepped to the card-rack, took the letter, put it in my pocket, and replaced it by a fac-simile, (so far as regards externals,) which I had carefully prepared at my lodgings; imitating the D– cipher, very readily, by means of a seal formed of bread.

"The disturbance in the street had been occasioned by the frantic behavior of a man with a musket. He had fired it among a crowd of women and children. It proved, however, to have been without ball, and the fellow was suffered to go his way as a lunatic or a drunkard. When he had gone, D-came from the window, whither I had followed him immediately upon securing the object in view. Soon afterwards I bade him farewell. The pretended lunatic was a man in my own pay.

"But what purpose had you," I asked, in replacing the letter by a fac-simile? Would it not have been better, at the first visit, to have seized it openly, and departed?"

"D–," replied Dupin, "is a desperate man, and a man of nerve. His hotel, too, is not without attendants devoted to his interests. Had I made the wild attempt you suggest, I might never have left the Ministerial presence alive. The good people of Paris might have heard of me no more. But I had an object apart from these considerations. You know my political prepossessions. In this matter, I act as a partisan of the lady concerned. For eighteen months the Minister has had her in his power. She has now him in hers; since, being unaware that the letter is not in his possession, he will proceed with his exactions as if it was. Thus will he inevitably commit himself, at once, to his political destruction. His downfall, too, will not be more precipitate than awkward. It is all very well to talk about the facilis descensus Averni; but in all kinds of climbing, as Catalani said of singing, it is far more easy to get up than to come down. In the present instance I have no sympathy –at least no pity –for him who descends. He is the monstrum horrendum, an unprincipled man of genius. I confess, however, that I should like very well to know the precise character of his thoughts, when, being defied by her whom the Prefect terms 'a certain personage,' he is reduced to opening the letter which I left for him in the card-rack."

"How? did you put any thing particular in it?"

"Why –it did not seem altogether right to leave the interior blank –that would have been insulting. D–, at Vienna once, did me an evil turn, which I told him, quite good-humoredly, that I should remember. So, as I knew he would feel some curiosity in regard to the identity of the person who had outwitted him, I thought it a pity not to give him a clue. He is well acquainted with my MS., and I just copied into the middle of the blank sheet the words–

–Un dessein si funeste, S'il n'est digne d'Atree, est digne de Thyeste.

They are to be found in Crebillon's 'Atree.'"