Vigenere cipher – polyalphabetic cipher

As it uses multiple alphabets to generate the ciphertext.

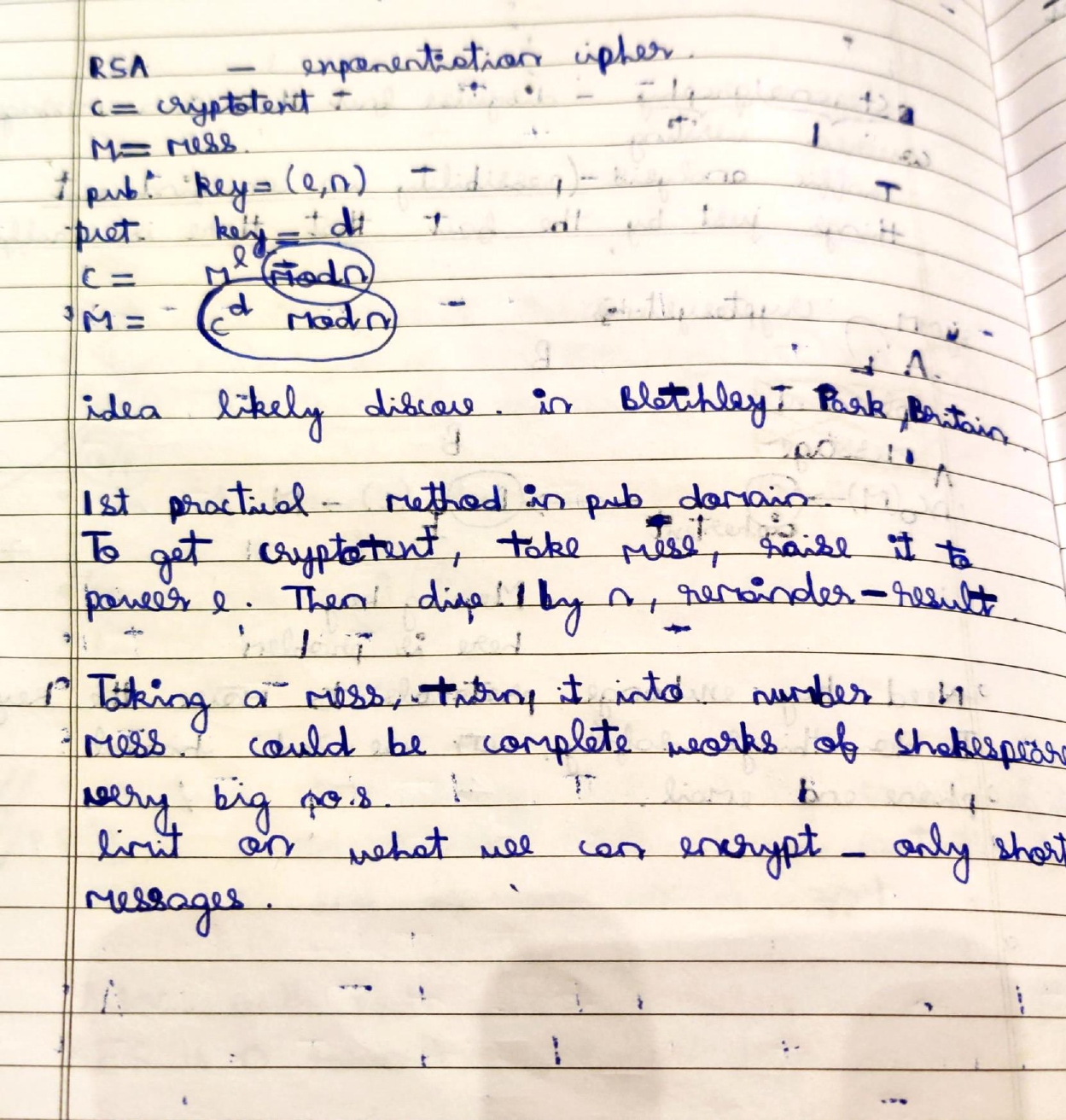
Length of key – period of cipher

When end of key reached ,key starts over.

Vigenere – uses a table called tableau

Repetitions – provide a means for cryptanalysts to attack a cipher.

RSA



One time pad – It can in principle be unbreakable

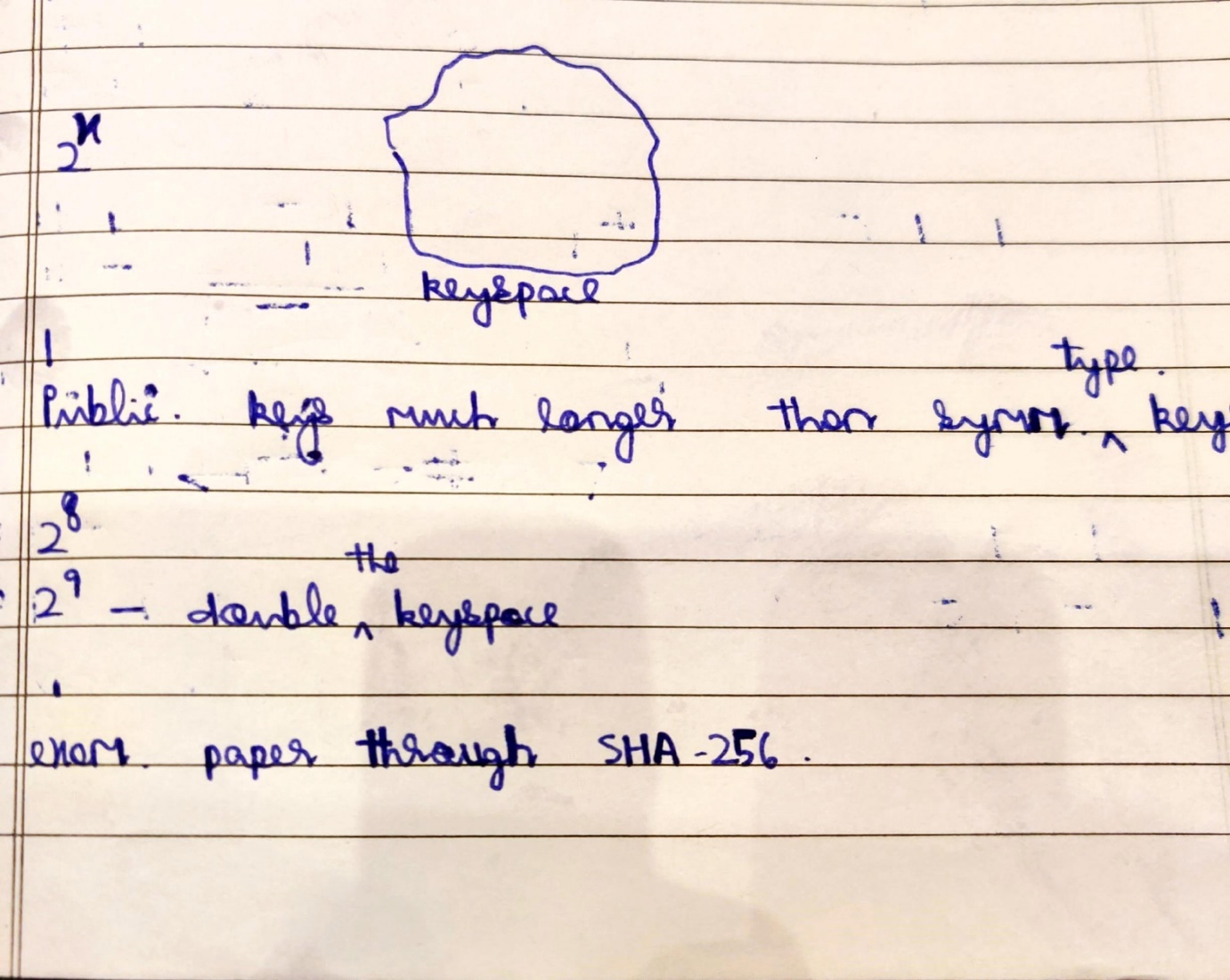
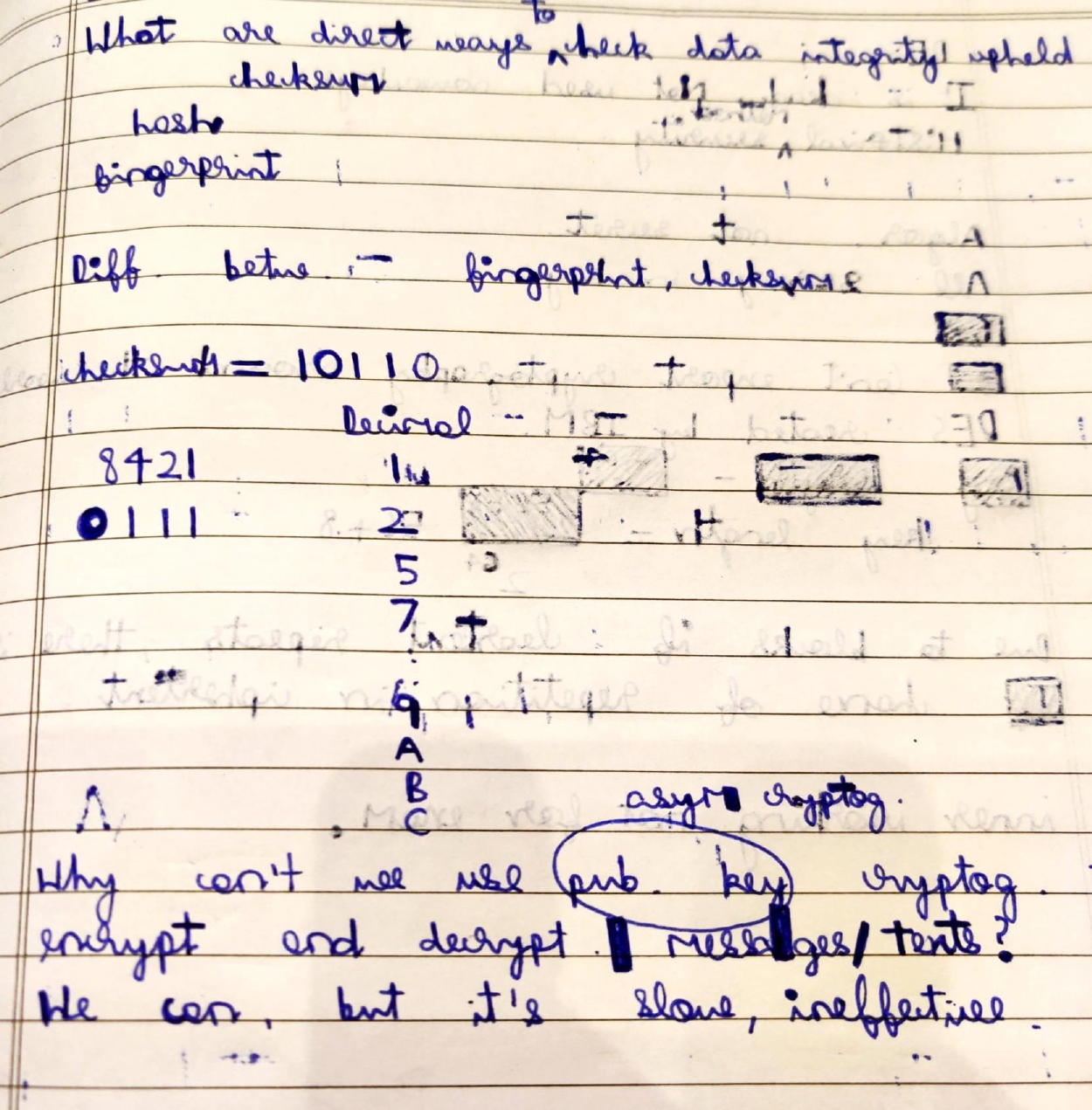
Variant of Vigenère cipher with key as long as plaintext chosen at random and doesn’t repeat.

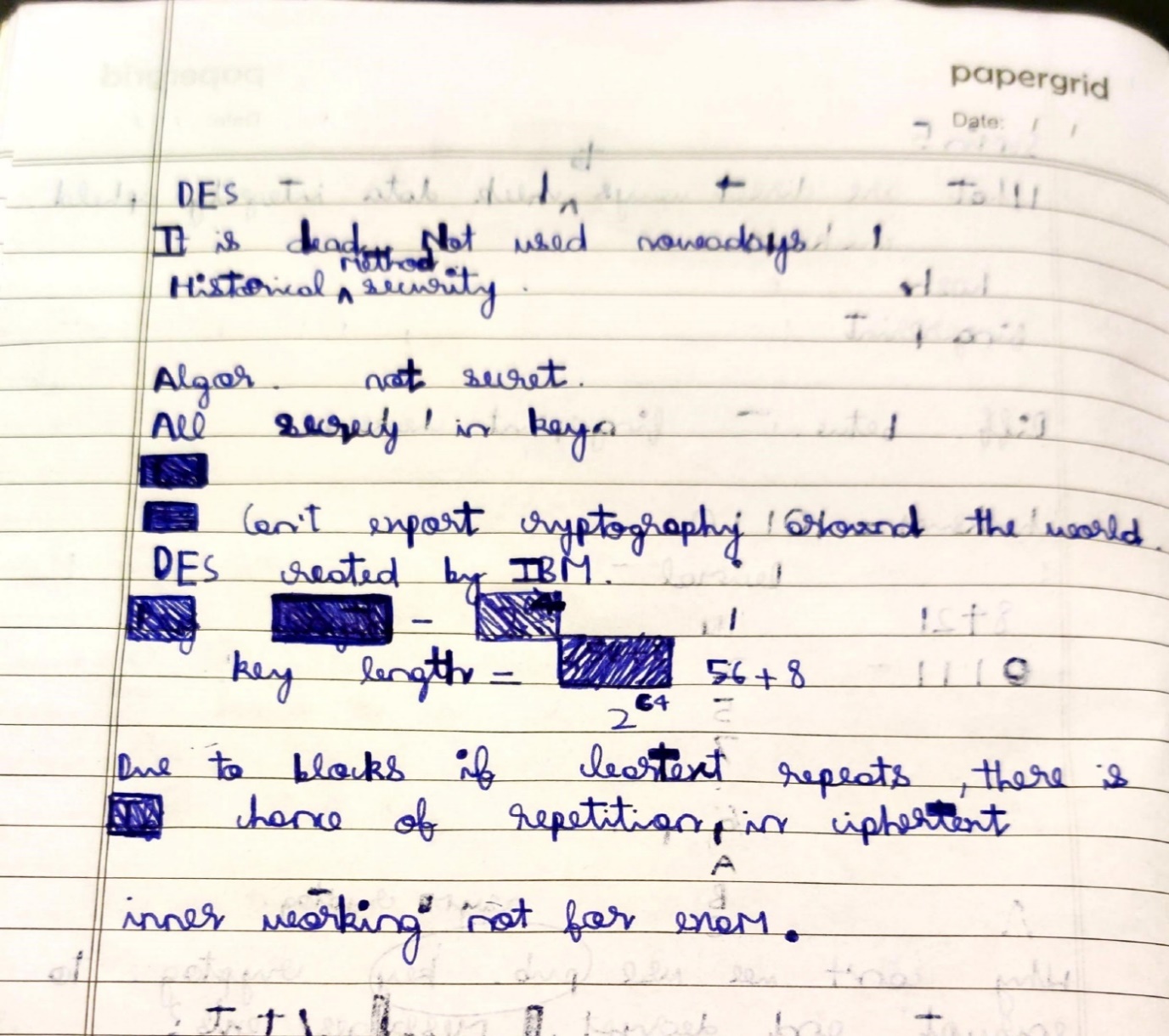
**Key Requirements**:

* + **Length**: The key must be at least as long as the plaintext.
  + **Randomness**: The key must be truly random, not just pseudorandom.
  + **Uniqueness**: The key must be used only once (hence the name "one-time pad") and then discarded.
  + **Secrecy**: The key must be kept completely secret.

\A screen shot of a presentation

Description automatically generated





DES is bit oriented.

Input , output ,key each 64 bits long. Sets of 64 bits – blocks.

AES is bit oriented

Uses key of 128 ,192 or 256 bits(usually 256)

RSA uses exponentiation and is asymmetric cipher.

 A symmetrical algorithm with keyspace up to 2256 → AES,

A symmetrical algorithm with key length of 64 bits → DES,

A symmetrical  encryption algorithm and substitutional cipher that can in principle be unbreakable → One time pad

An asymmetrical algorithm invented in the 1970s → RSA