Computational Cryptography
CMPUT 299

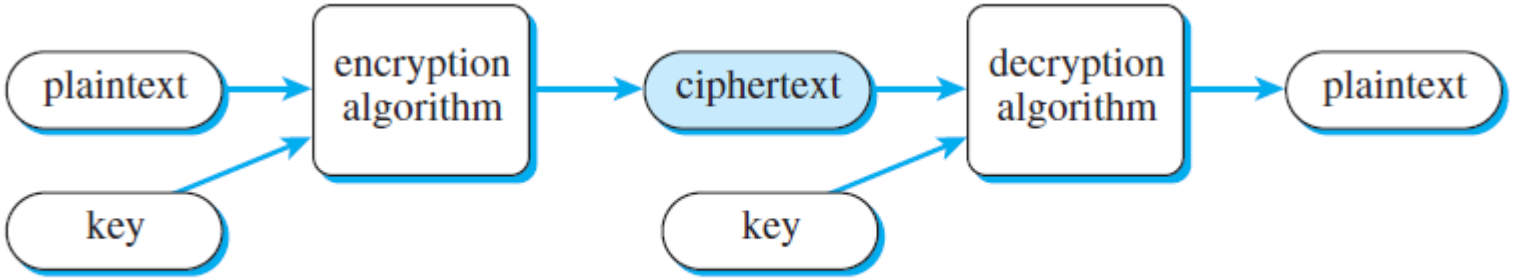
Review

Cryptography

- Encryption (with a key):
  - transposition cipher
  - substitution cipher
  - Caesar cipher
  - affine cipher
  - Vigenere cipher
  - RSA
- Decryption (with a key) = inverse of encryption
- Cryptanalysis = decryption without a key

Encryption and decryption

Encryption and decryption with a key



Code breaking (hacking)

- Brute force: try all possible keys
  - manual: Caesar cipher (25 possible keys)
  - computerized: can check millions of keys
  - substitution cipher: over 10^{26} possible keys
- Letter frequency analysis
- Word dictionary matching
- Guessing parts of ciphertext
- Spying

Transposition cipher: encryption

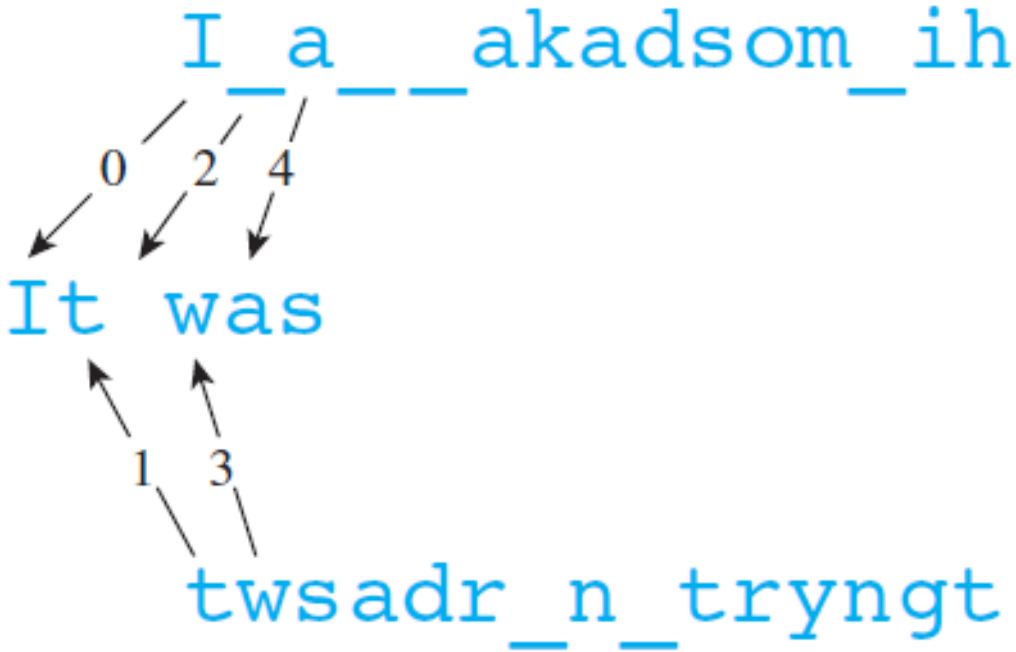
Original	It was a dark and stormy night
Even	I _ a _ _ a k a d s o m _ i h
Odd	t w s a d r _ n _ t r y n g t

Break up the plaintext into even and odd characters

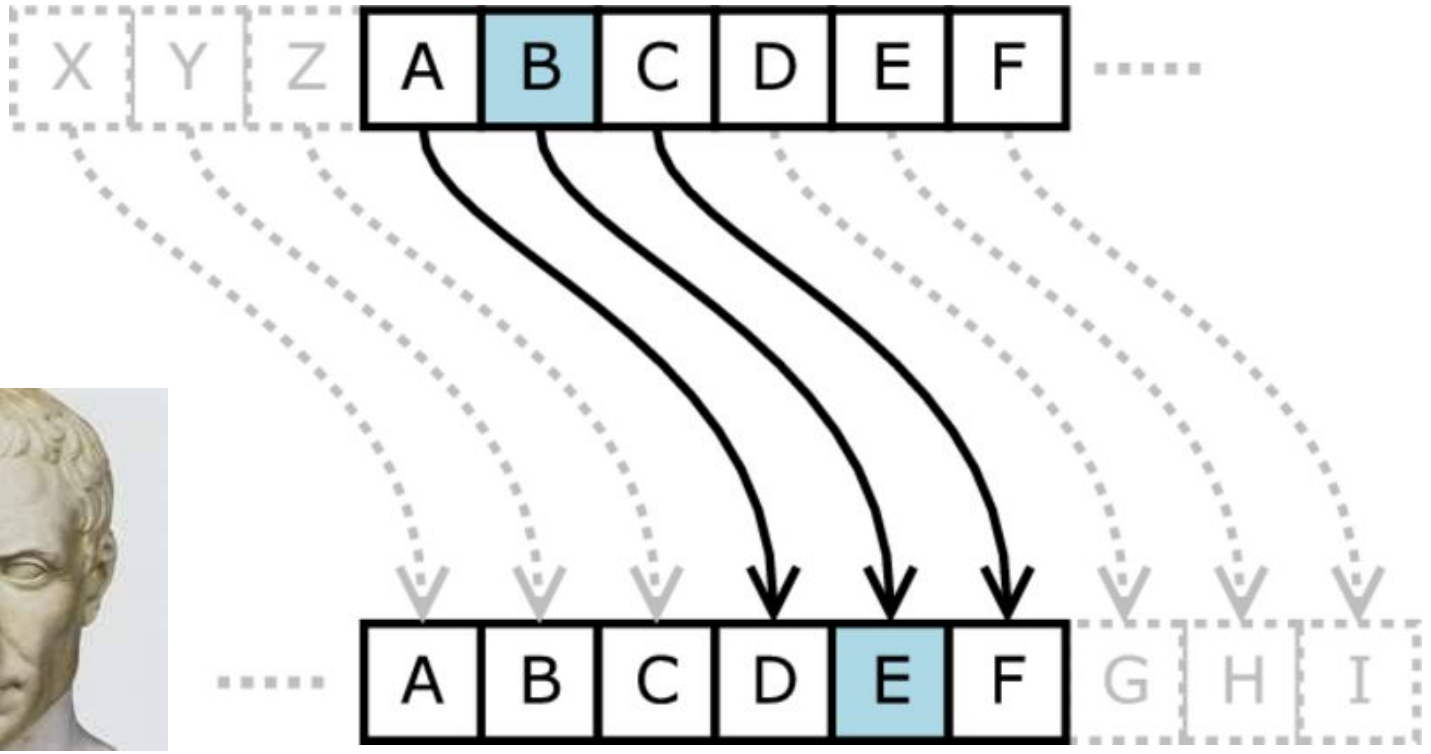
twsadr_n_tryngt + I_a__akadsom_ih

Combine the even and odd parts to make the ciphertext

Transposition cipher: decryption



Caesar cipher



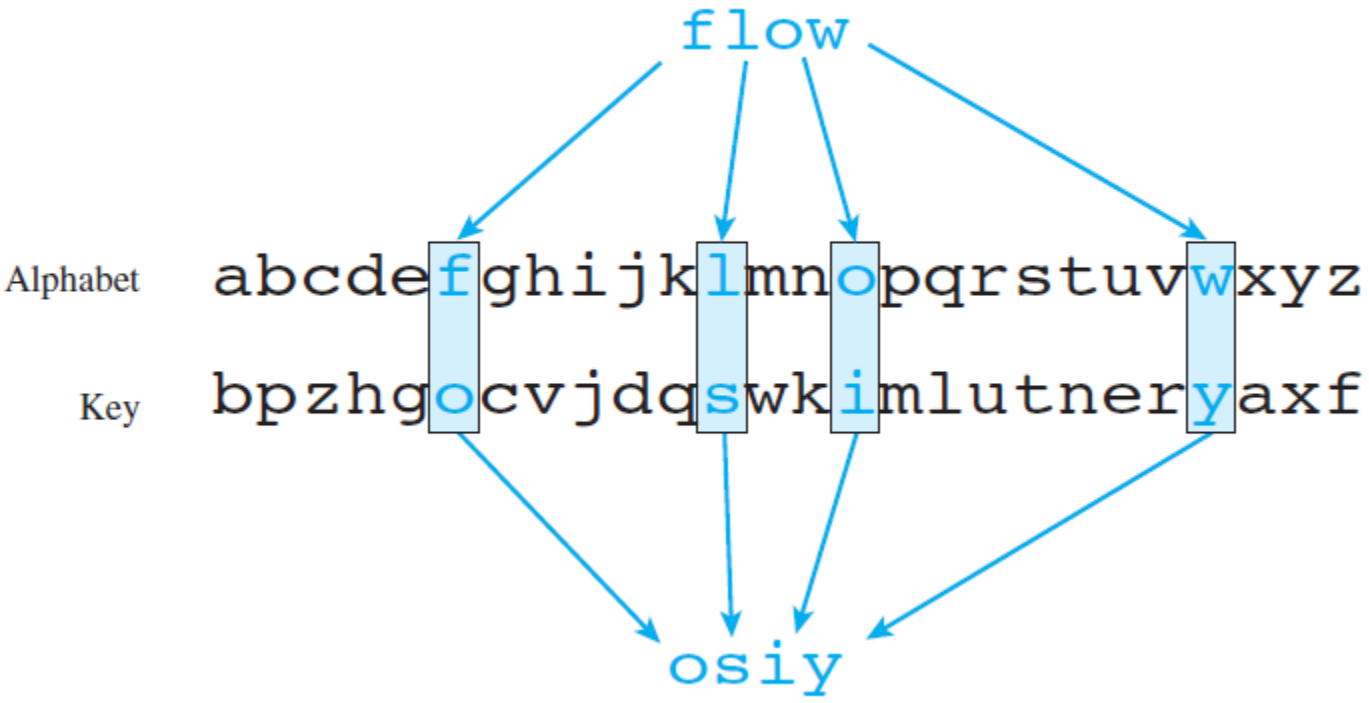
Hacking Caesar with Brute Force

Key #0: GUVF VF ZL FRPERG ZRFFNTR.
Key #1: FTUE UE YK EQODQF YQEEMSQ.
Key #2: ESTD TD XJ DPNCPE XPDDLRP.
Key #3: DRSC SC WI COMBOD WOCCKQO.
Key #4: CQRB RB VH BNLANC VNBBJPN.
Key #5: BPQA QA UG AMKZMB UMAAIOM.
Key #6: AOPZ PZ TF ZLJYLA TLZZHNL.
Key #7: ZNOY OY SE YKIXKZ SKYYGMK.
Key #8: YMNX NX RD XJHWJY RJXXFLJ.
Key #9: XLMW MW QC WIGVIX QIWWEKI.
Key #10: WKLV LV PB VHFUHW PHVVDJH.
Key #11: VJKU KU OA UGETGV OGUUCIG.
Key #12: UIJT JT NZ TFDSFU NFTTBHF.
Key #13: THIS IS MY SECRET MESSAGE.
Key #14: SGHR HR LX RDBQDS LDRRZFD.
Key #15: RFGQ GQ KW QCAPCR KCQQYEC.
Key #16: QEFP FP JV PBZOBQ JBPPXDB.
Key #17: PDEO EO IU OAYNAP IAOOWCA.
Key #18: OCDN DN HT NZXMZO HZNNVBZ.
Key #19: NBCM CM GS MYWLYN GYMMUAY.
Key #20: MABL BL FR LXVKXM FXLLTZX.
Key #21: LZAK AK EQ KWUJWL EWKKSYW.
Key #22: KYZJ ZJ DP JVTIVK DVJJRXV.
Key #23: JXYI YI CO IUSHUJ CUIIQWU.
Key #24: IWXH XH BN HTRGTI BTHHPVT.
Key #25: HVWG WG AM GSQFSH ASGGOUS.

Affine cipher

- multiplicative cipher + Caesar cipher
- each letter is encrypted using a formula
- $E(x) = (ax + b) \bmod m$
- $D(x) = a^{-1} (x - b) \bmod m$
  - a^{-1} is the modular inverse of a
  - $aa^{-1} \bmod m = 1$
- a and $|\Sigma|$ must be relatively prime
  - Σ is the alphabet; $|\Sigma|$ is its size
- the number of possible keys is $< |\Sigma|^2$

Substitution cipher



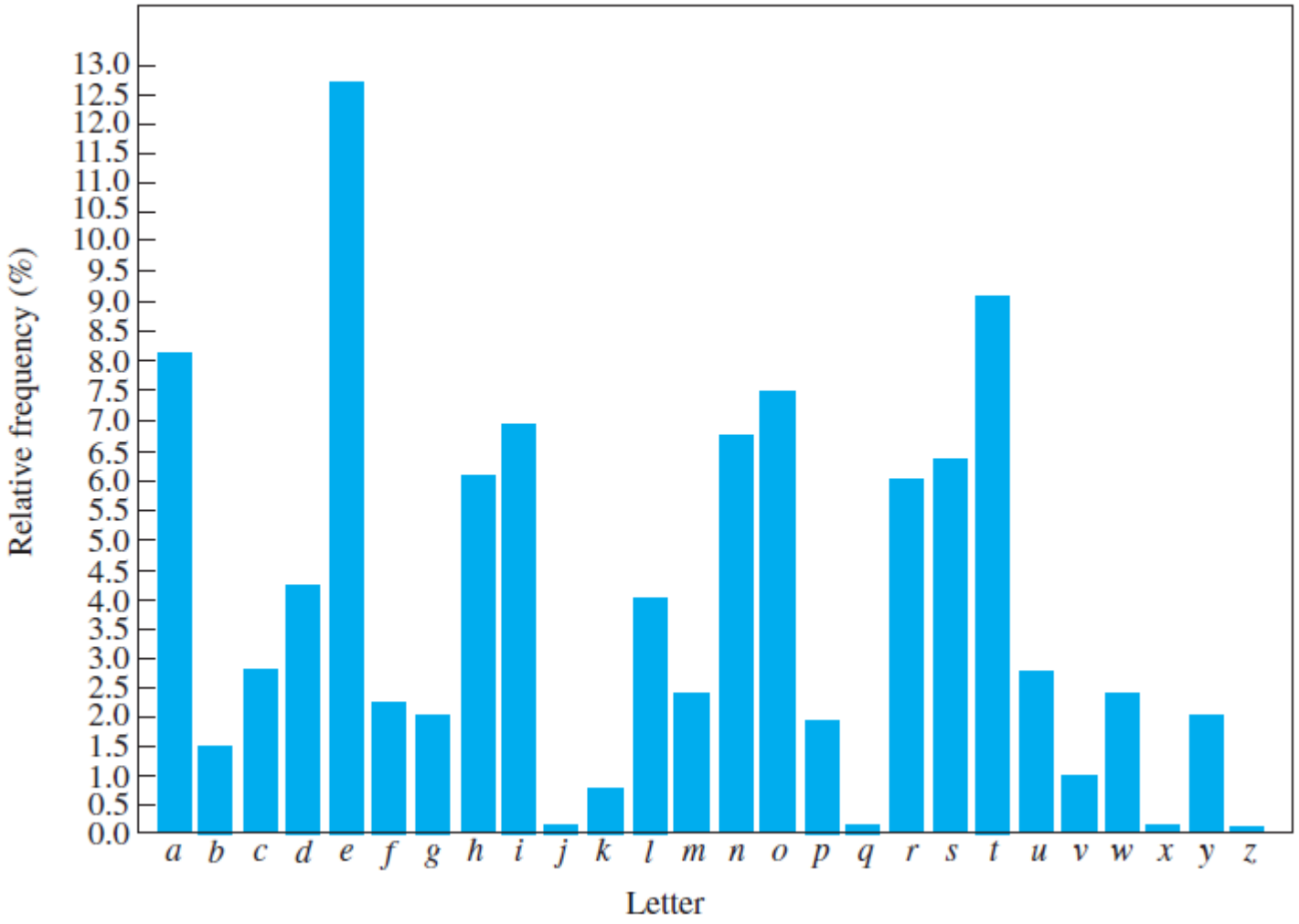
Creating a Key

- Random key is hard to remember
- Base key on a word or a short phrase
- For example, “JULIUS CAESAR”
- Remove repeated letters: JULISCAER
- Add remaining letters:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

JULISCAERTVWXYZBDFGHKMNOPQ

Relative letter frequencies



Cryptanalysis of a ciphertext

- match relative letter frequencies in ciphertext to those in a large plain text
- letter doubles: *ss ee tt ff ll mm oo*
- 2-letter words: *of to in it is*
- 3-letter words: *the and*
- frequent bigrams: *th er he*
- guess words/phrases
- consonants vs. vowels

Regular Expression Summary

Regular Expression	Interpretation
.	match any character
[abc]	match *a* or *b* or *c*
[^abc]	match any character other than
[abc]+	match one or more occurrences
[abc]*	match zero or more occurrences
(*regex*)	create a capture group

Playfair cipher

Encode each bigram with another bigram.

EG

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

XD

Vigenere cipher

- Vigenere is like Caesar with multiple keys
- The keyword is aligned with the message:

```
Message:  thesunandthemoon
     Key:  KINGKINGKINGKING
  Cipher:  DPRYEVNTXBUKWWBT
```

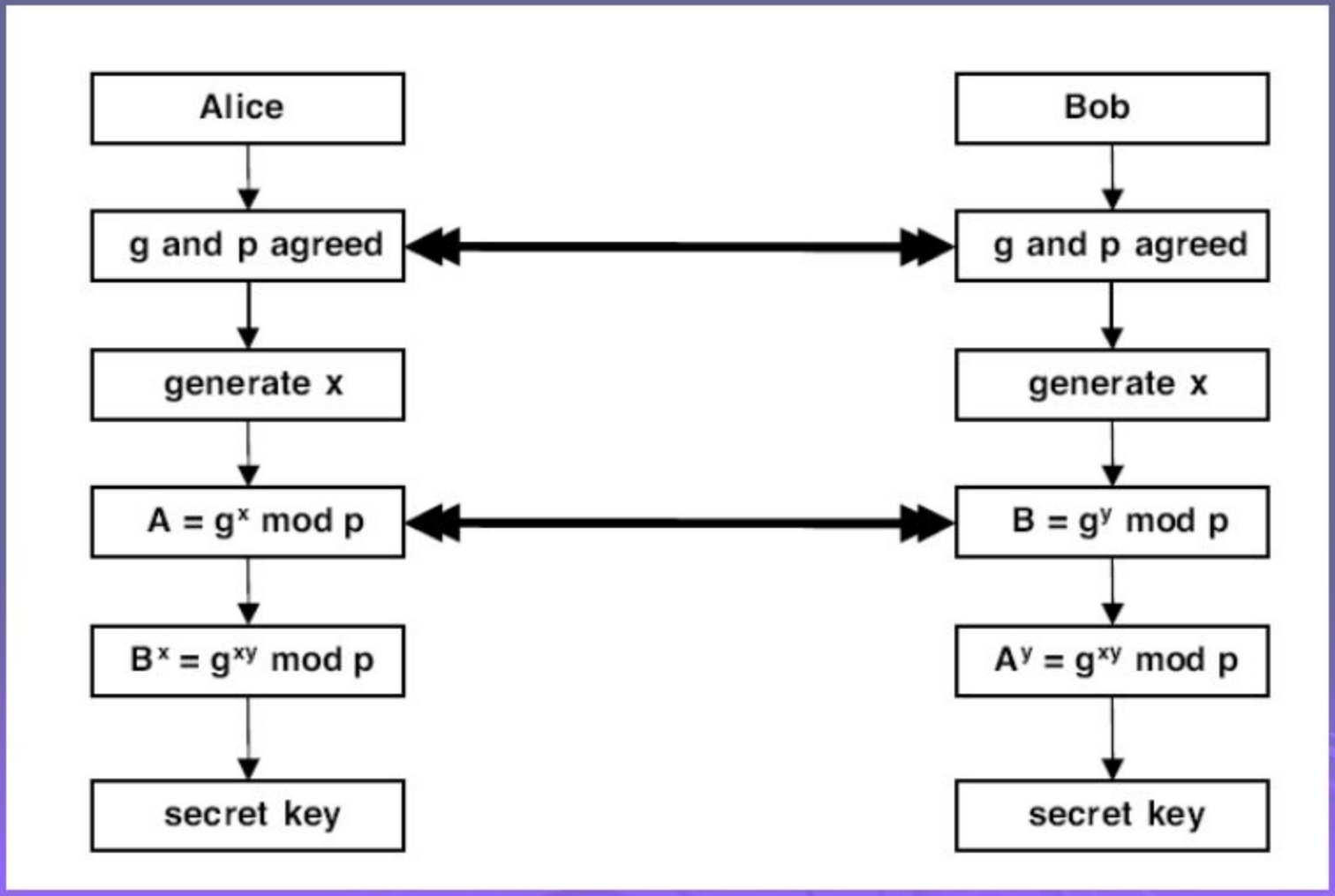
- Each ciphertext letter is “the sum” of the keyword letter and the plaintext letter:

$$C_i = (M_i + K_i) \bmod 26$$

One-time pad

- Vigenere cipher with a very long key
- Provably unbreakable, provided that:
  - the key is as long as the message
  - the key is truly random
  - the key is never used more than once
- Problems:
  - truly random numbers are not easy to generate
  - secure exchange of a long and un-reusable key

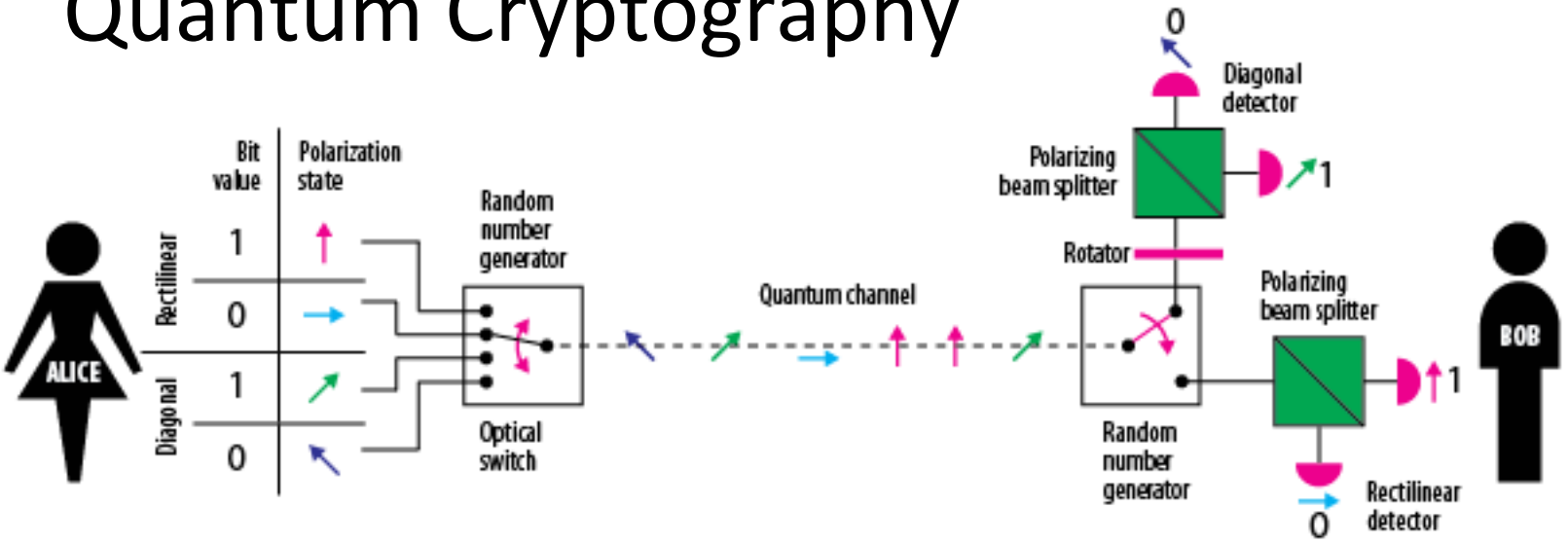
Diffie-Hellman Key Exchange



RSA cipher

- Key generation:
  - select primes p, q; calculate n = pq
  - select e that is co-prime with (p-1)(q-1)
  - calculate d as a modular inverse of e mod (p-1)(q-1)
  - public key = {e,n}; private key = {d,n}
- Encode blocks of text as integers < n
- Encryption: $C = M^e \bmod n$
- Decryption: $M = C^d \bmod n$

Quantum Cryptography



Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	ALICE tells BOB which bits to keep		✔		✔		✔	✔	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

Source: UNS Nice (France), Department of Physics