cphbusiness

COPENHAGEN BUSINESS ACADEMY





Security, Spring 2019

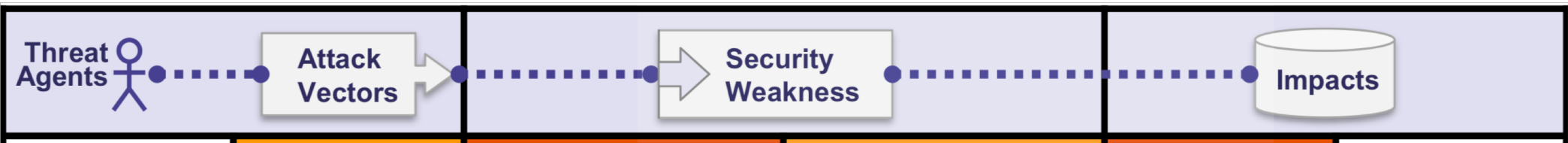
OWASP top 10, 2013 & 2017

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Detection

A3:2017-Sensitive Data Exposure

(See page 9 of OWASP 2017)



App. Specific	Exploitability: 2	Prevalence: 3	Detectability: 2	Technical: 3	Business ?
Rather than directly attacking crypto, attackers steal keys, execute man-in-the-middle attacks, or steal clear text data off the server, while in transit, or from the user's client, e.g. browser. A manual attack is generally required. Previously retrieved password databases could be brute forced by Graphics Processing Units (GPUs).		Over the last few years, this has been the most common impactful attack. The most common flaw is simply not encrypting sensitive data. When crypto is employed, weak key generation and management, and weak algorithm, protocol and cipher usage is common, particularly for weak password hashing storage techniques. For data in transit, server side weaknesses are mainly easy to detect, but hard for data at rest.		Failure frequently compromises all data that should have been protected. Typically, this information includes sensitive personal information (PII) data such as health records, credentials, personal data, and credit cards, which often require protection as defined by laws or regulations such as the EU GDPR or local privacy laws.	

GDPR

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in today's data-driven world. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.

GDPR - Increased Territorial Scope (extraterritorial applicability)

- All companies processing personal data of EU residents
- Non-EU businesses
- Businesses offering goods to EU residents

GDPR – Data Subject Rights

- Breach notifications are mandatory (72 hours)
- Right to access
- Right to be forgotten
- Data portability in a ‘commonly use and machine readable format’

GDPR - Penalties

- Up to 4% of annual global turnover
- €20.000.000
- Whichever is greater!

- Revenue of facebook was $40.654.000.000 in 2017, so the turnover was much higher
- 4% of revenue is €1.391.738.381

GDPR – Privacy by default

- The conditions for consent have been strengthened, and companies are no longer able to use long illegible terms and conditions full of legalese.
- It must be as easy to withdraw consent as it is to give it.

GDPR – Privacy by design

- At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.
- Controllers should
  - hold and process only the data absolutely necessary for the completion of its duties
  - limit the access to personal data to those needing to act out the processing.

GDPR – Data Protection Officers

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest.

What is personal data?

Personal data is any information that relates to an identified or identifiable living individual.

For example:

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone)*;
- an Internet Protocol (IP) address;
- a cookie ID*;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

Data controller

The data controller determines the purposes for which and the means by which personal data is processed.

So, if your company/organisation decides ‘why’ and ‘how’ the personal data should be processed it is the data controller.

Data processor

The data processor processes personal data only on behalf of the controller. The data processor is usually a third party external to the company.

E.g. A payroll company, many IT service companies

Exercise 0

Design a system for handling signatures for new parties.

- You can sign up for at most one party
- Signatures are binding – they can’t be withdrawn

Encrypting your information

Is like putting your valuables in a safe.

It is a second layer in case your house is broken into.

Base64 encoding

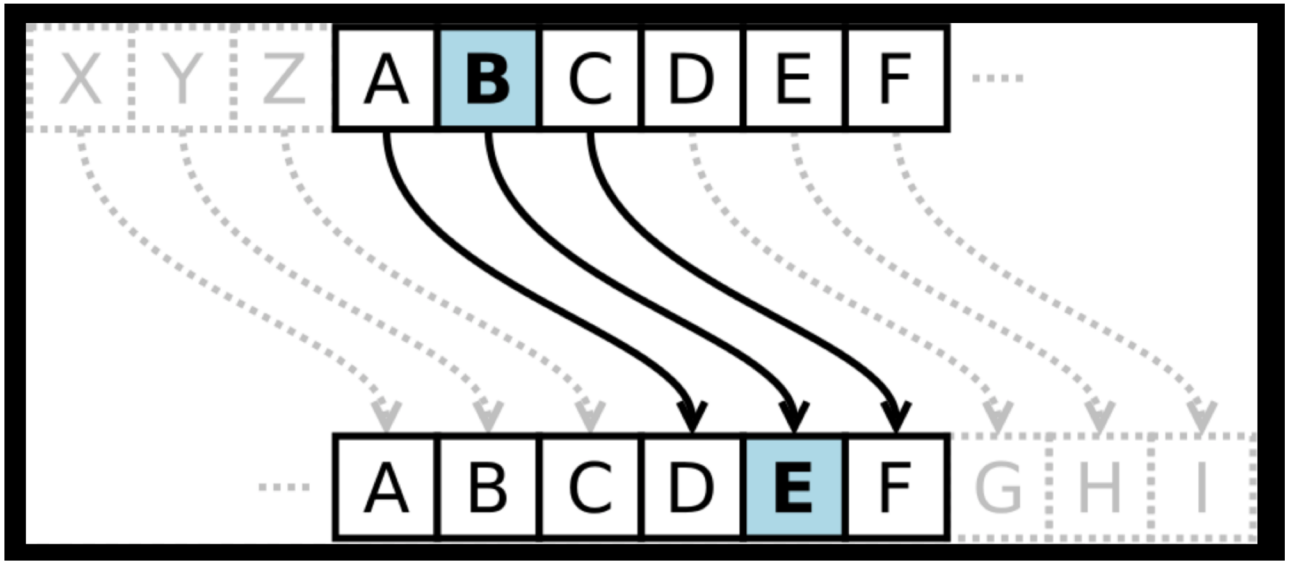
Often we need to store binary information as characters (e.g. emails with attachments)

Base64 encode/decode is one way to do this.

Java has support for this – look in exercise 1.

Cesar rot code

Such an old method it is not clear it was ever used.

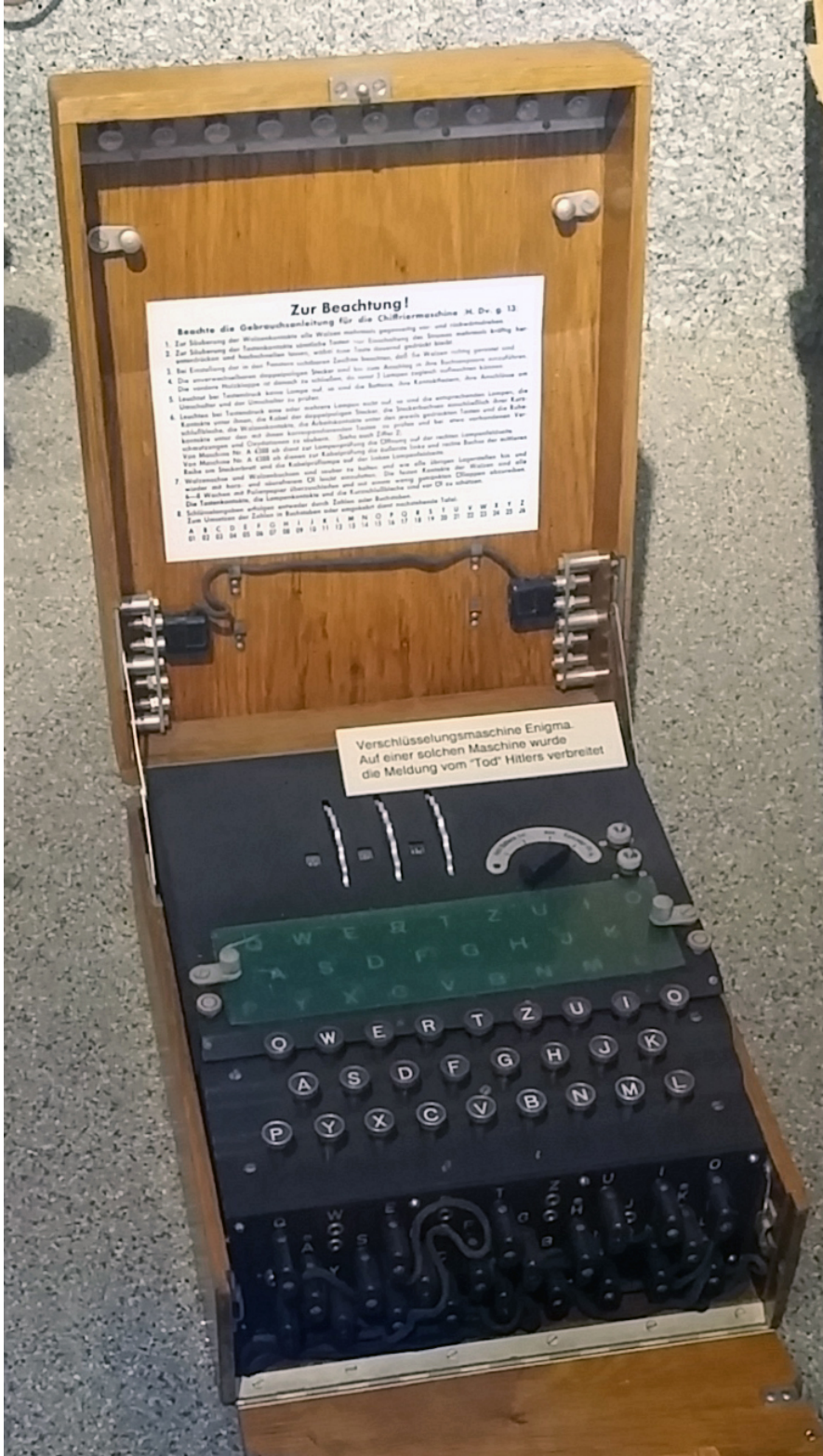


Rot-3

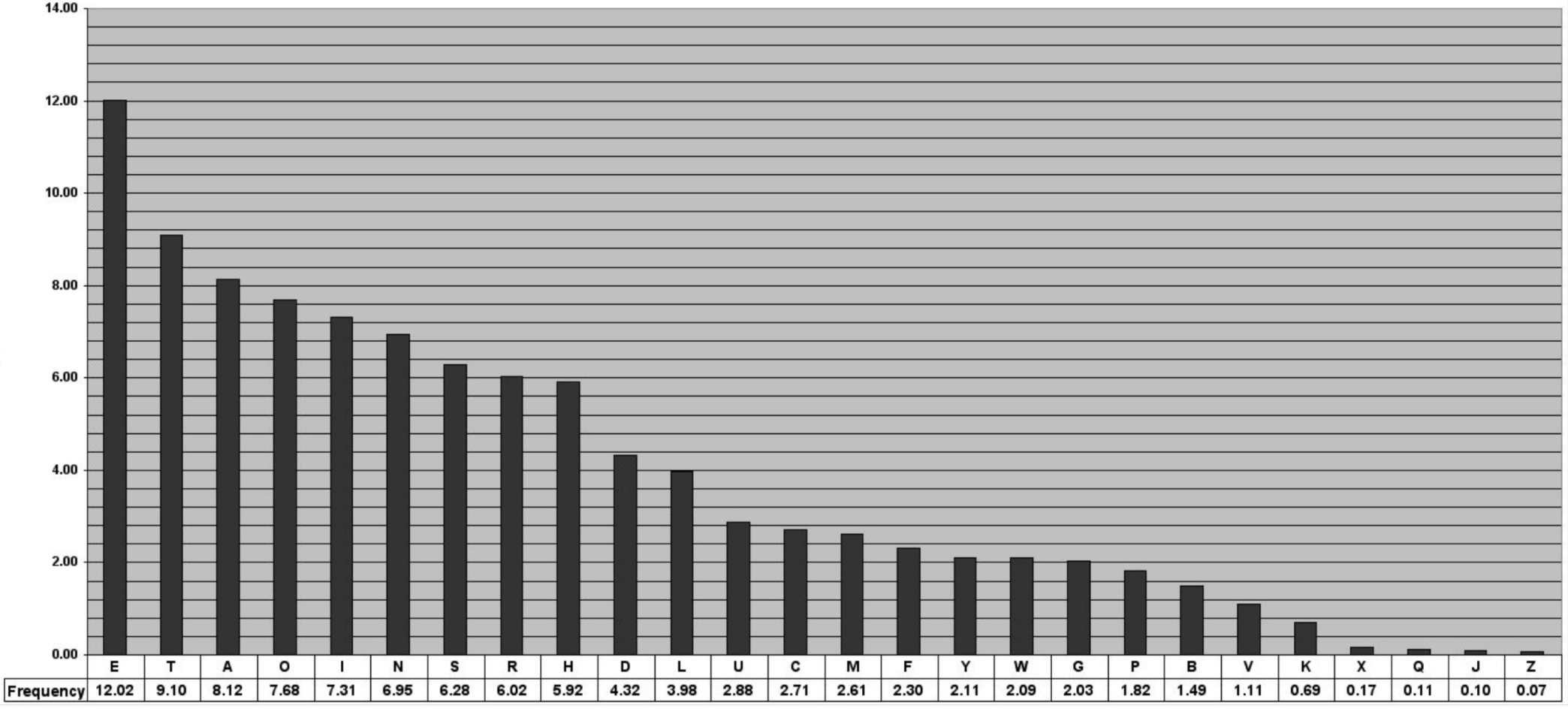
Crack the code in exercise 1.

Substitution ciphers

- Simple substitution
- Polyalphabetic substitution
  - More alphabets
- Polygraphic substitution
  - Larger groups of characters
- The one-time pad
  - Use a book

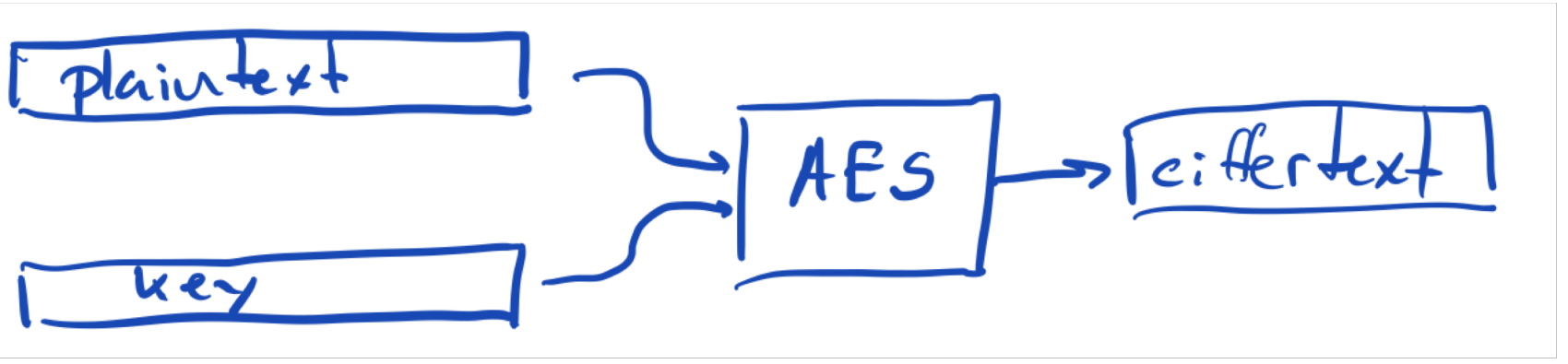


Using frequencies



	E	T	A	O	I	N	S	R	H	D	L	U	C	M	F	Y	W	G	P	B	V	K	X	Q	J	Z
Frequency	12.02	9.10	8.12	7.68	7.31	6.95	6.28	6.02	5.92	4.32	3.98	2.88	2.71	2.61	2.30	2.11	2.09	2.03	1.82	1.49	1.11	0.69	0.17	0.11	0.10	0.07

AES algorithm



The heart of the algorithm can “only” encrypt blocks which are 128, 196, or 256 bits long

(16, 24, or 32 bytes)

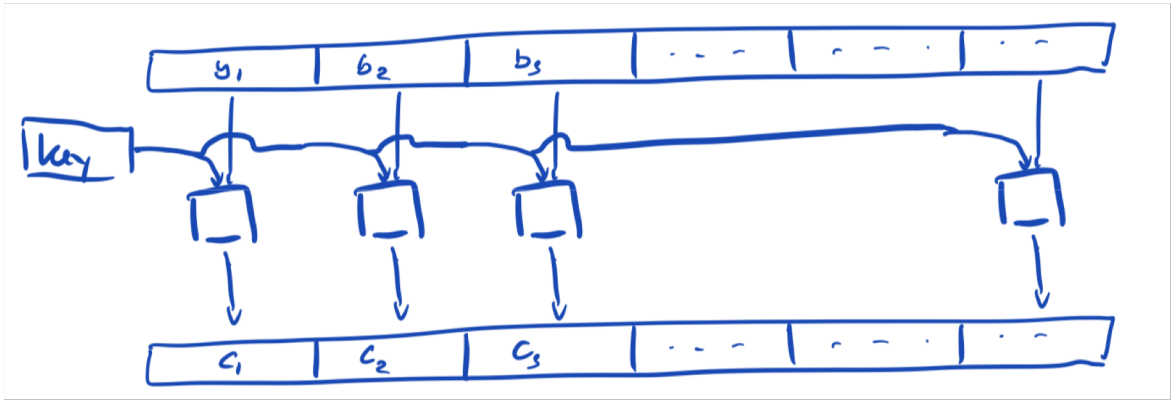
((Long session and drawing on the whiteboard))

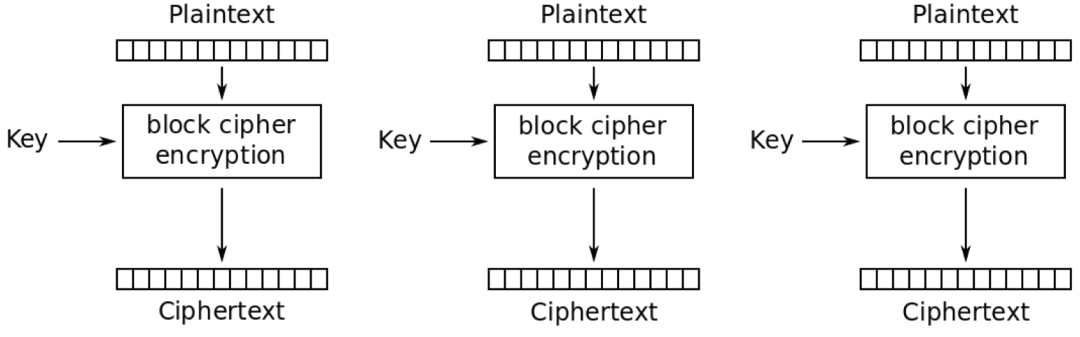
To make it work on real data, we need to

1. break the plain text into *blocks* and
2. encrypt each *block*. There is one stupid way, and many good ways to do this

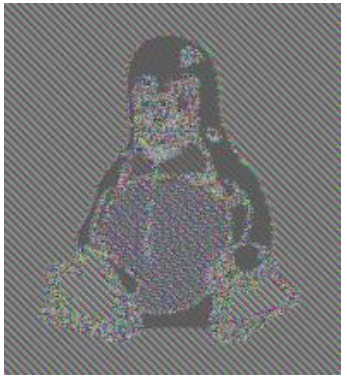
The stupid way - Electronic Codebook (ECB)

Do not encode each block using the same key



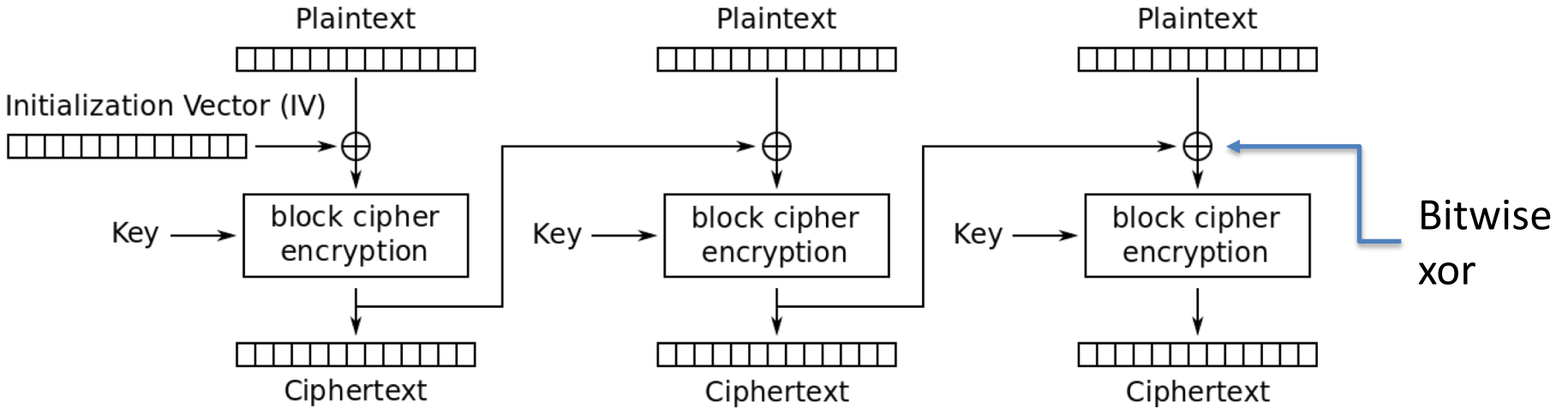


Electronic Codebook (ECB) mode encryption

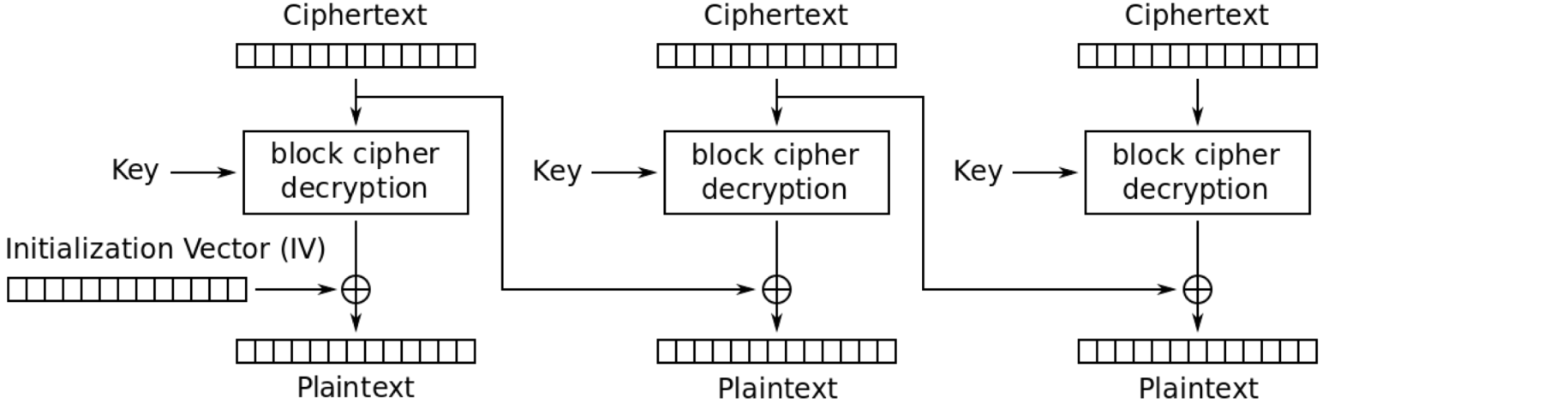


cphbusiness

Cipher Block Chaining (CBC)



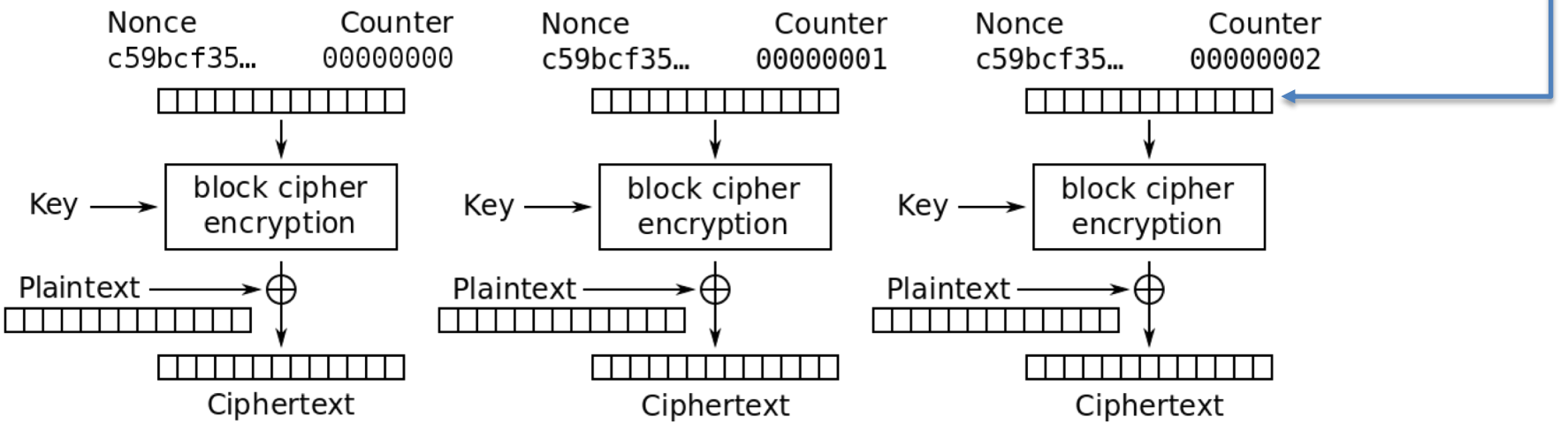
Cipher Block Chaining (CBC) mode encryption



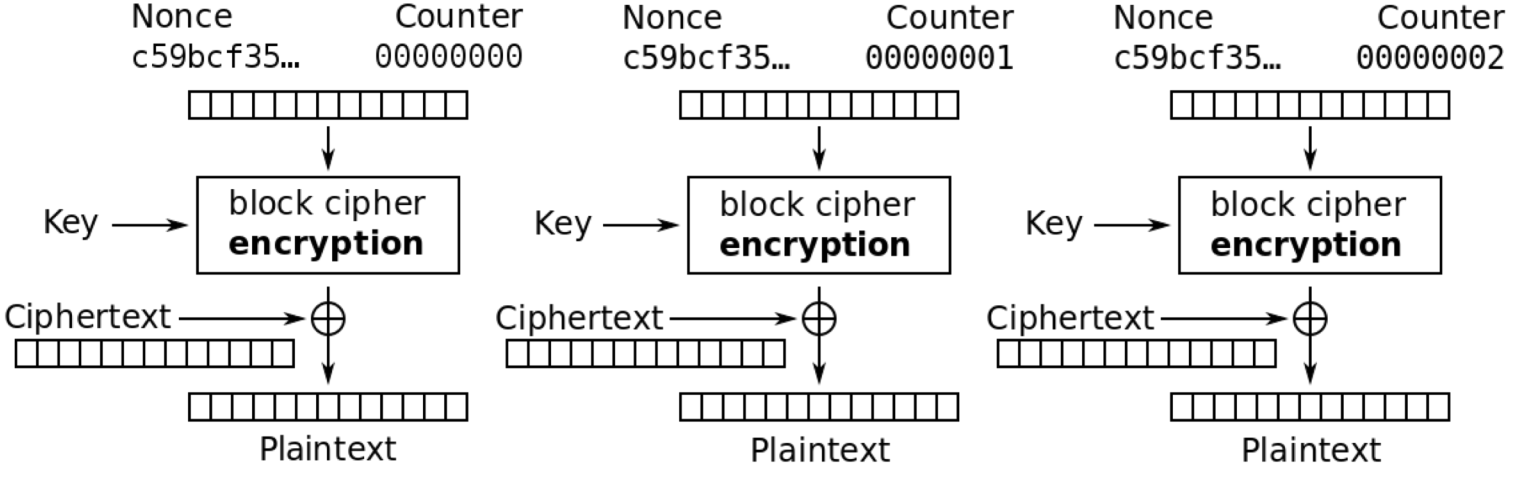
Cipher Block Chaining (CBC) mode decryption

Counter (CTR)

Secret & blockcount combined using xor or other mechanism



Counter (CTR) mode encryption



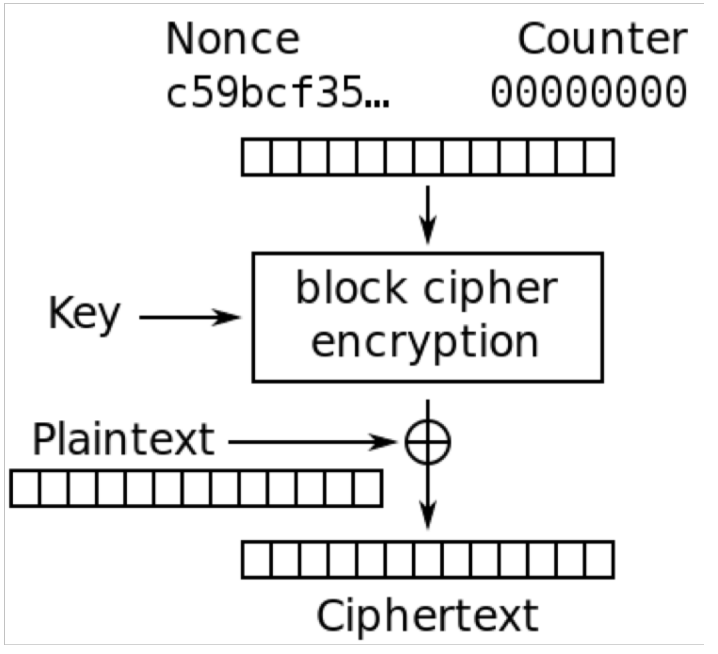
Counter (CTR) mode decryption

There are Java libraries for it all

And they are easy to use wrong.

There are three inputs

- Plaintext
- Key
- Nonce (NumberOnce)



The Nonce

Is generated by a good random generator, **saved to disk** to be used later for decryption.

See sample code for this

The key

Has to be 128 (or 196 or 256) bits.

Is mostly *generated* from a password.

We will not go into password hashing now.

See the sample code for how to generate a 128 bit key from arbitrary password.