

The slide features decorative blue lines in the corners. In the top-left, three parallel lines form an L-shape. In the bottom-left, three parallel lines extend horizontally and then angle downwards. In the bottom-right, three parallel lines angle upwards from the bottom edge.

# Java Cryptography Architecture

SOPHIE PFISTER

## Context

- Kühne *et al.* (2017)

and their parameters. We have implemented a compiler that translates a CRYSL ruleset into a context- and flow-sensitive demand-driven static analysis. The analysis automatically checks a given Java or Android app for violations of the CRYSL-encoded rules.

We empirically evaluated our ruleset through analyzing 10,001 Android apps. Our results show that misuse of cryptographic APIs is still widespread, with 96% of apps containing at least one misuse. However, we observed fewer of the misuses that were reported in previous work.



## Context

- Cryptography libraries lack usability.
- API misuse leads to security vulnerabilities.

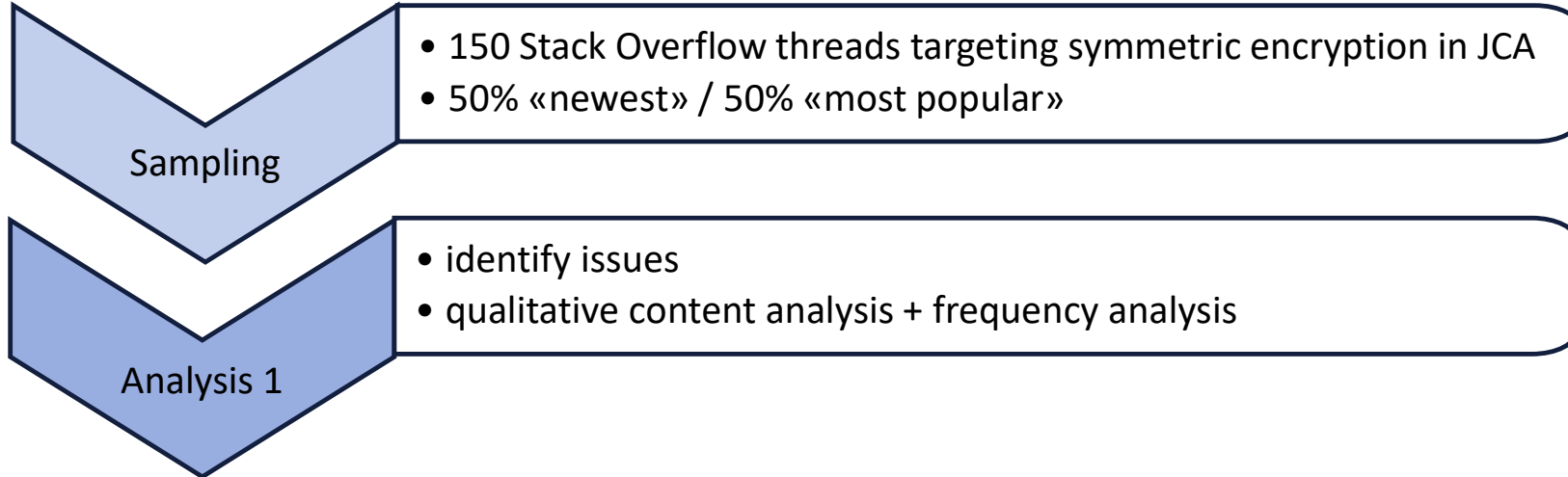
→ unsafe applications!



## Research Questions

1. What **issues** do programmers face when implementing symmetric encryption using the JCA library?
2. What **security risks** are present on Stack Overflow referring to the implementation of symmetric encryption using JCA library?
3. To what extent are these **linked to** missing or inadequate **documentation**?

# Methodology





# Analysis 1

- Summarizing
- Classification 1: Technical Aspects
- Classification 2: Requirements

# Analysis 1: Technical Aspects

Cipher Object Instantiation

Parameters Generation

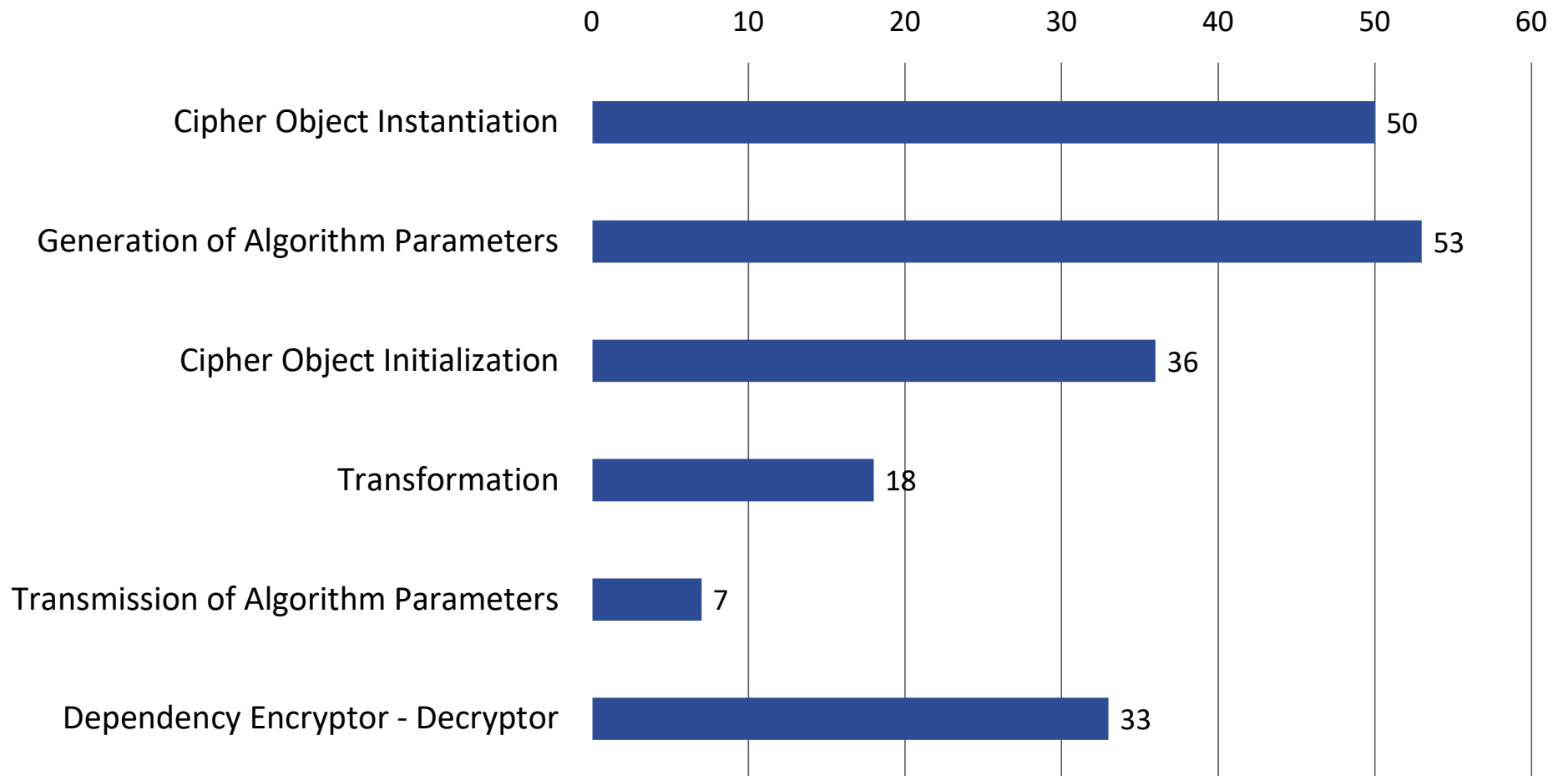
Cipher Object Initialization

Transformation

Parameter Transmission

Dependency Encryptor - Decryptor

## Records Classified Regarding Technical Aspects (N = 219)







## Analysis 1: Technical Aspects

<b>Total</b>	<b>197 issues</b>	<b>(90%)</b>
Generation of Algorithm Parameters:	53 issues	(24.2%)
• Key Derivation	36 issues	(16.5%)
Cipher Object Instantiation:	50 issues	(22.8%)
• Encryption Mode & Padding	40 issues	(18.3%)



# Analysis 1: Requirements

Use Cases (Functional Requirements)

Performance

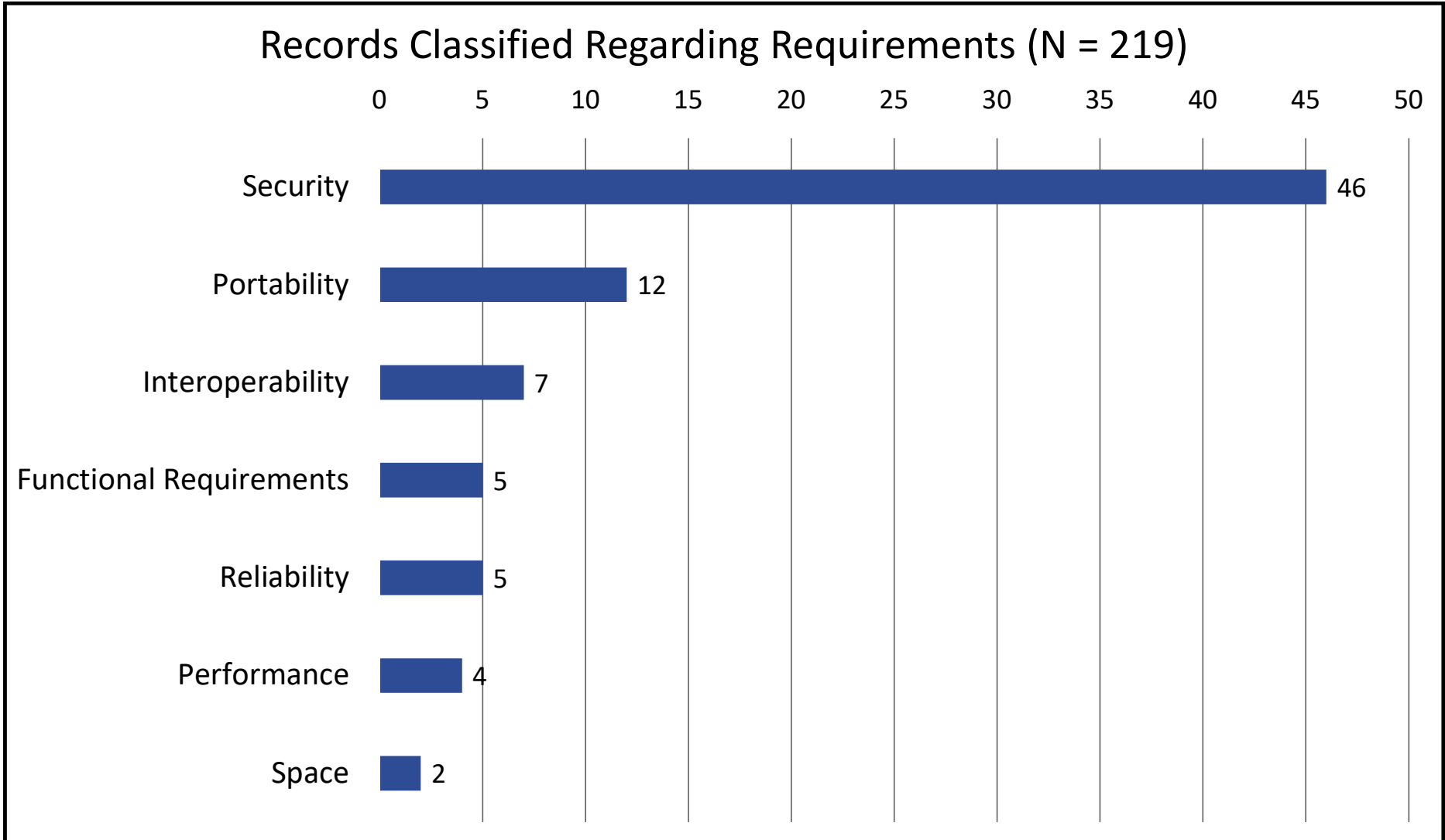
Space

Reliability

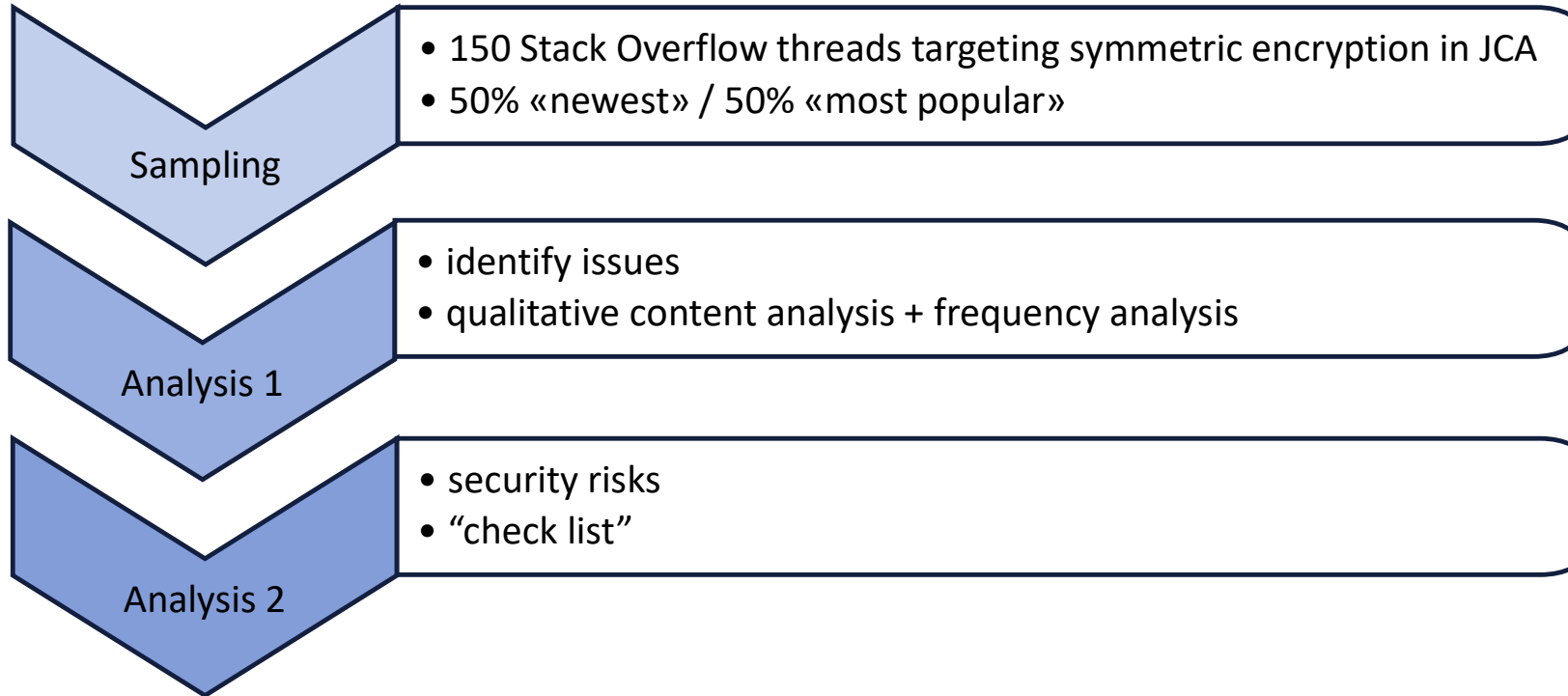
Interoperability


Portability

Security



# Methodology





## Analysis 2: Check List

- Deriving rules from existing sets
  - CRYLOGGER tool for dynamic security risk tracking
  - CogniCrypt compiler for static security risk tracking

## Analysis 2: Security Rules

Cipher Object Instantiation

Parameters Generation

Cipher Object Initialization

Parameter Transmission



## Analysis 2: Checklist

4 Checklists:

- Question – Code
- Question – Text
- Answer – Code
- Answer – Text

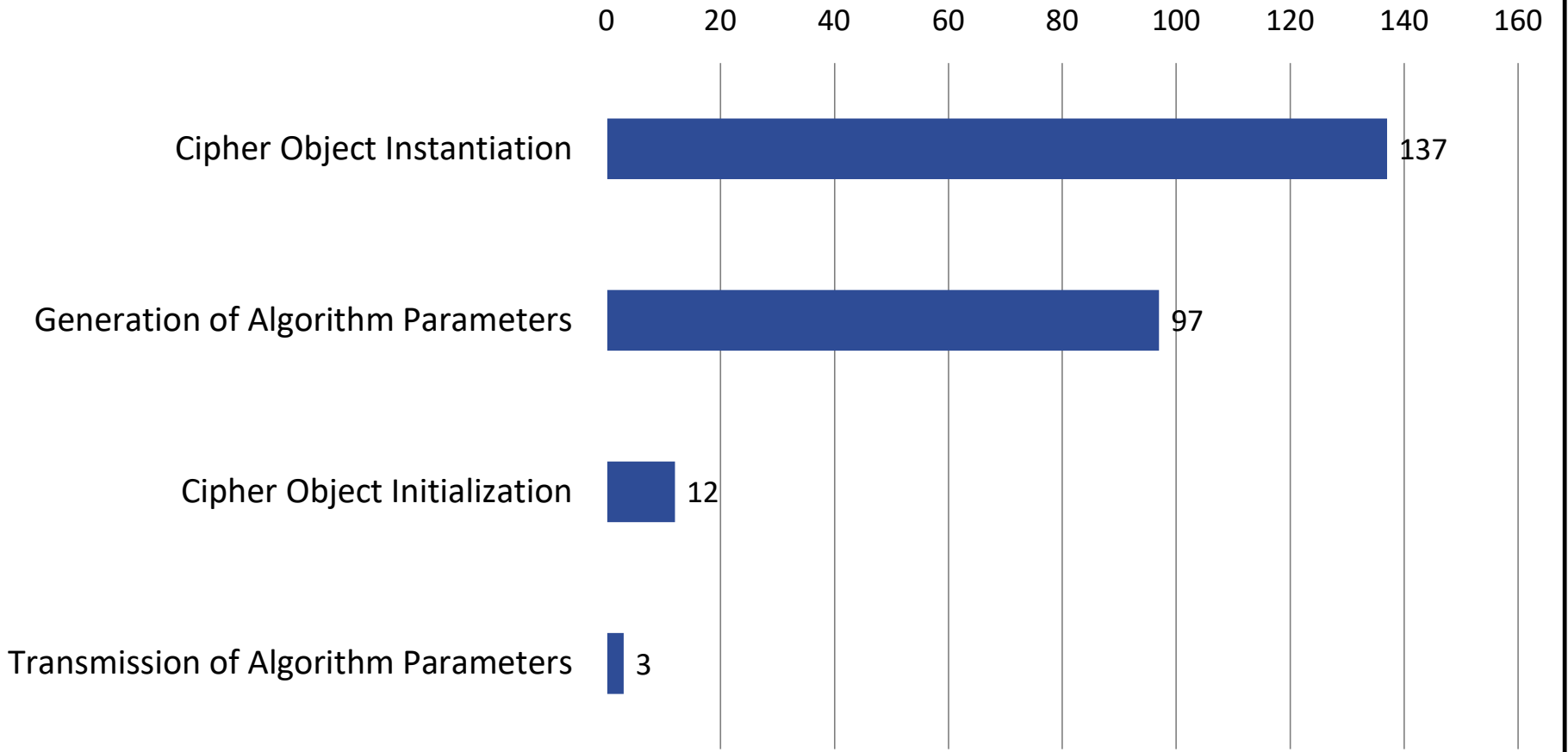
## Analysis 2: Results

- 150 question posts and 84 answer posts
- 331 security risks

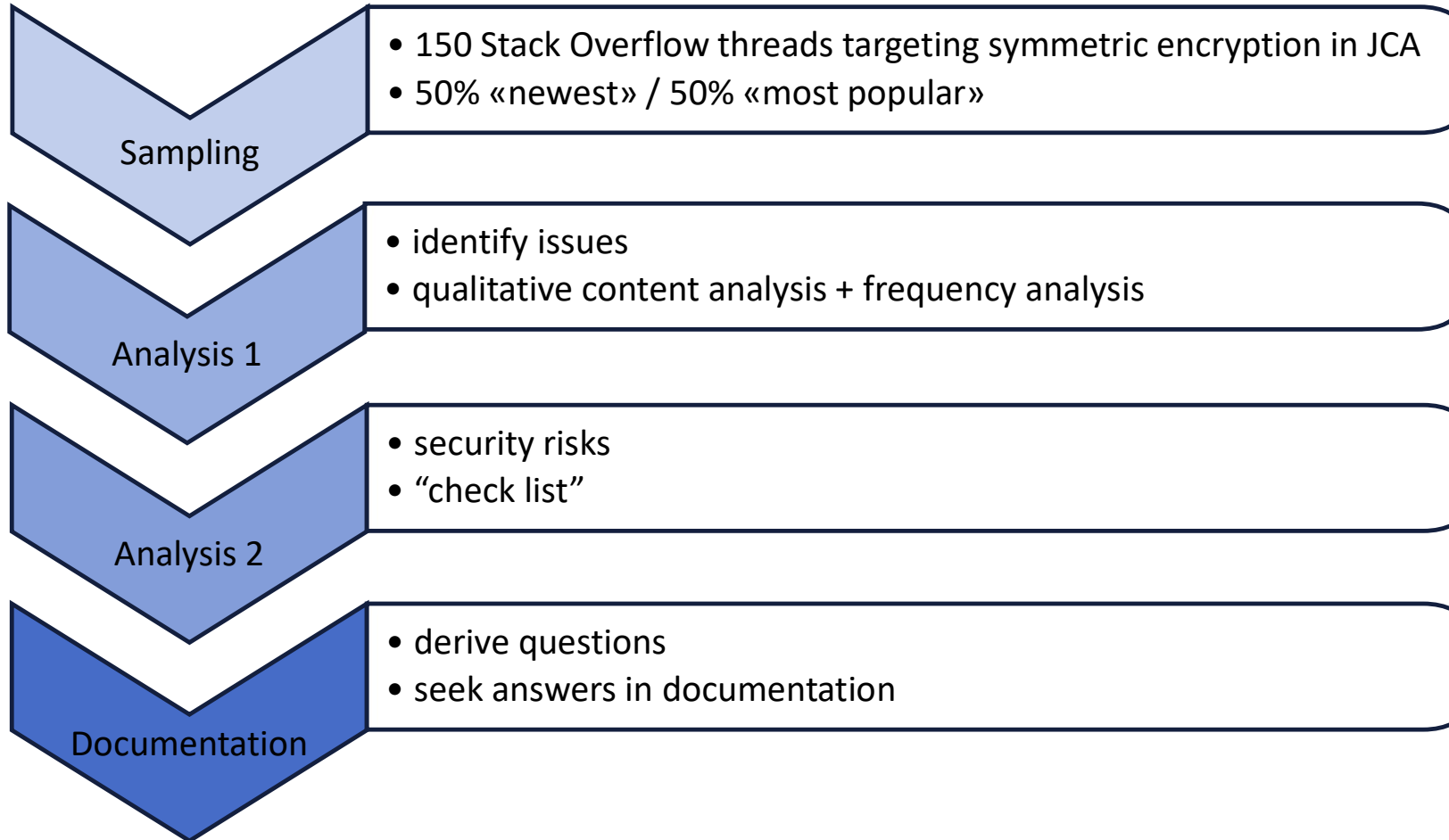
	Code	Text
Question	249	38
Answer	35	9



### Security Risks in Question Related Code



# Methodology





## Questions

- based on results from former analyses
- How many threads are targeted by a question?  
→ Priority
- 2 Lists:
  - «General Questions»
  - «Questions to Documentation»

# Questions - to Documentation

Question	Priority
→ What happens if I do not specify the IV although it is required?	9
→ How can I derive a key from a password?	7
→ What is the default value if I do not specify padding?	6
→ What kind of parameters do I have to pass to the decryption methods (update / doFinal)?	6
→ Which of the provided key derivation functions are standardized?	6

- default behavior
- (password based) key derivation
- method overloads

# Questions - General

Question	Priority
→ Which encryption modes are safe?	113
→ What are security requirements for the key?	43
→ What requirements must the IV / nonce meet to be safe?	37
→ Which input data and specifications must be equal for encryption and decryption?	27
→ Which symmetric encryption algorithms are safe to use?	24
→ What are requirements for safe password based key derivation?	15

- security related
- dependency encryptor - decryptor

# Questions - General

Question	Priority
→ What encryption modes require padding?	9
→ Which encryption modes do require an IV or nonce?	6
→ What is the required size for an IV?	5
→ What key sizes are supported by AES?	4
→ What does an IV do during encryption?	4

- encryption mode
- initialization vector
- key

## Questions

- Total: 66 Questions
- 10 questions unanswered
- 13 answers are unclear, incomplete, or misleading

*“Advanced Encryption Standard as specified by NIST in FIPS 197. Also known as the Rijndael algorithm by Joan Daemen and Vincent Rijmen, AES is a 128-bit block cipher supporting keys of 128, 192, and 256 bits.”*



## Unanswered Questions

- How can I specify PKCS#7 padding in Java?
- What properties does AES-256 require?
- Which symmetric algorithms are safe?





## General Observations

- examples are not working (incomplete)
- platform / provider issue  
→ decreases portability



# Conclusion





# What **issues** do programmers face ...?

## Tasks / Properties:

- (password based) key derivation
- key storage / transmission
- initialization vector
- encryption mode

## API Related Issues

- platforms and providers
- overloaded methods, `update (...)` vs. `doFinal (...)`

## Programmer Related Issues

- lack of (domain) knowledge



## What **security risks** are present... ?

- unsafe encryption mode (ECB, CBC)
- static values for key and initialization values
- unsafe key derivation procedure



## ... issues **linked to** ... **documentation?**

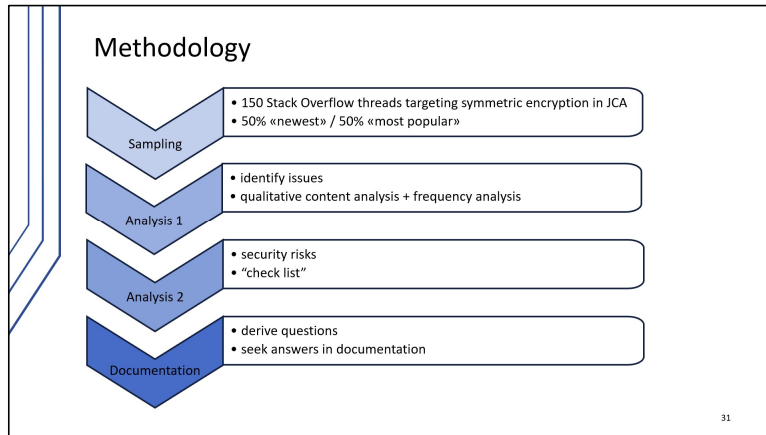
- 65% of questions are answered by documentation
- “higher priority” questions are answered
- Yet, the quality could be improved by
  - providing working code examples
  - linking trusted resources
  - adding security hints / warnings



## Conductive Thoughts

- Do programmers read documentation?
- API usability is very complex.
- Implementing cryptography requires expertise.

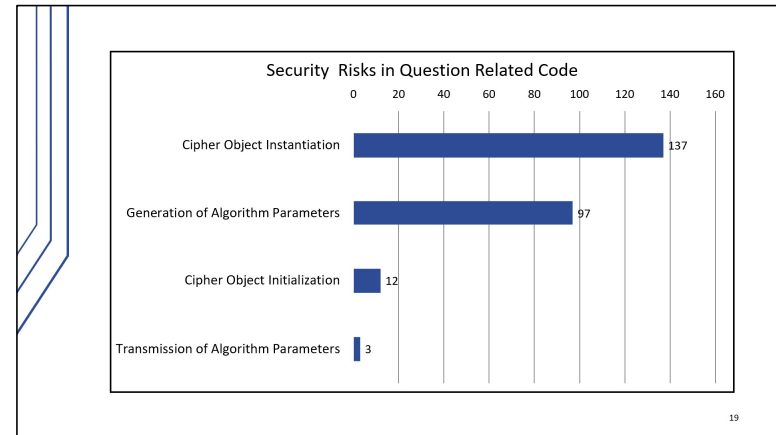
# Summary



### Analysis 1: Technical Aspects

<b>Total</b>	<b>197 issues</b>	<b>(90%)</b>
Generation of Algorithm Parameters:	53 issues	(24.2%)
• Key Derivation	36 issues	(16.5%)
Cipher Object Instantiation:	50 issues	(22.8%)
• Encryption Mode & Padding	40 issues	(18.3%)

10



### Questions - General

Question	Priority
Which encryption modes are safe?	113
Which key derivation functions are safe?	40
What requirements must an IV / nonce / salt meet to be safe?	37
Which input data and specifications must be equal for encryption and decryption?	27
Which symmetric encryption algorithms are safe to use?	24
What are requirements for a safe password based key derivation function?	15

34