The purpose of this survey is to understand how people use Java cryptography APIs. We are a group of researchers from TU Darmstadt, Germany, who work on creating tools to help developers use cryptography in their Java applications. We want to understand what cryptography tasks you usually perform, any difficulties you face, and what would help you use cryptography more correctly/efficiently.Answering this survey should not take more than 10 minutes of your time. Your participation is anonymous and voluntary.Please note that you should use a modern web-browser with JavaScript enabled. The following browsers should work: IE8+, Firefox 4+, Safari 3+, and Chrome 2+.If you have any questions or comments about this survey, please contact Sarah Nadi (nadi@st.informatik.tu-darmstadt.de)

What is your current occupation?

- ○ Undergraduate student (1)
- ○ Graduate student (2)
- ○ Academic Researcher (3)
- ○ Industrial Researcher (4)
- ○ Industrial developer (5)
- ○ Freelance developer (6)
- ○ Other (7) ____________________

How many years of Java development experience do you have?

- ○ < 1 year (1)
- ○ 1 - 2 years (2)
- ○ 2 - 5 years (3)
- ○ 6 - 10 years (4)
- ○ 11+ years (5)

How would you rate your background/knowledge about cryptography concepts such as encryption, digests, signatures, etc.? Note that this is knowledge from an end-user perspective and does not necessarily include understanding how the underlying mathematics work

- ○ Not knowledgeable - I do not know anything about cryptography (1)
- ○ Somewhat knowledgeable - I have a vague idea about the various areas of cryptography and what they are used for (2)
- ○ Knowledgeable - I am familiar with the various areas of cryptography and what they are used for (3)
- ○ Very knowledgeable - I know all/most areas of cryptography, the different available algorithms, and what they are used for (4)

How often do you need to use cryptography in the software you develop?

- ○ Never - I never I use cryptography in any of my development tasks (1)
- ○ Rarely - I use cryptography in less than 33% of my development tasks (2)
- ○ Occasionally - I use cryptography in more than 33% but less than 66% of my development tasks (3)
- ○ Frequently - I use cryptography in more than 66% of my development tasks (4)

If Never - I never use cryptog... Is Selected, Then Skip To End of Survey

What are the most common cryptography-related tasks you need in your applications? Rank the tasks where 1 is the most common task you do. Add your own tasks as needed. Leave task rank empty if you do not use it, but do not skip ranks (i.e., a ranking of 1,2,4 instead of 1,2,3 is invalid)

_______ Store/authenticate user names and passwords (1)
_______ Encrypt file (2)
_______ Secure connections and communications (3)
_______ Transfer files securely (4)
_______ Other (5)
_______ Other (6)
_______ Other (7)
_______ Other (8)
_______ Other (9)

Did you use Java Cryptography libraries/APIs before?

○ Yes (1)

○ No (2)

If No Is Selected, Then Skip To Further comments

Please rank the Java cryptographic libraries/APIs below according to your frequency of use where 1 is most used. Additional libraries you use can be added in the other fields. Leave option blank if you do not use this library/API, but do not skip ranks (i.e., a ranking of 1,2,4 instead of 1,2,3 is invalid)

______ Java Cryptography Architecture (JCA) APIs (irrespective of provider) (1)
______ Lightweight Bouncy Castle API (2)
______ Other (3)
______ Other (4)
______ Other (5)
______ Other (6)
______ Other (7)

Thinking of your most-used API, ${q://QID9/ChoiceGroup/ChoiceWithLowestValue}, how would you rate its ease of use in terms of accomplishing your tasks correctly and securely?

○ Very hard to use (1)
○ Hard to use (2)
○ Easy to use (3)
○ Very easy to use (4)

Answer If Thinking of your most-used API,&nbsp;${q://QID9/ChoiceGroup/ChoiceWithLowestValue}, how would you rate its ease of use in terms of accomplishing&nbsp;your tasks correctly and securely? Very hard to use Is Selected Or Thinking of your most-used API,&nbsp;${q://QID9/ChoiceGroup/ChoiceWithLowestValue}, how would you rate its ease of use in terms of accomplishing&nbsp;your tasks correctly and securely? Hard to use Is Selected

What obstacles made it hard for you to learn and use ${q://QID9/ChoiceGroup/ChoiceWithLowestValue}? Obstacles can have to do with the API itself, with your background, with learning resources, etc. List the three most important obstacles, in order of importance (1 being the biggest obstacle). Please be more specific than the general categories mentioned here.

Answer If Thinking of your most-used API,&nbsp;${q://QID9/ChoiceGroup/ChoiceWithLowestValue}, how would you rate its ease of use in terms of accomplishing&nbsp;your tasks correctly and securely? Easy to use Is Selected Or Thinking of your most-used API,&nbsp;${q://QID9/ChoiceGroup/ChoiceWithLowestValue}, how would you rate its ease of use in terms of accomplishing&nbsp;your tasks correctly and securely? Very easy to use Is Selected

What features of your most-used API, ${q://QID9/ChoiceGroup/ChoiceWithLowestValue}, makes it ${q://QID12/ChoiceGroup/SelectedChoices}?

Thinking of when you have a new cryptography-related task to implement in your software (e.g., storing passwords, encrypting emails, etc.), do you ever have difficulties with the following?

	Never (1)	Rarely (2)	Occasionally (3)	Frequently (4)	Don't know (5)
Identify the correct algorithm (e.g., AES vs DES) to use (1)	❍	❍	❍	❍	❍
Identify which concepts (e.g., encryption vs hashing) to use (2)	❍	❍	❍	❍	❍
Identify which Java API to use (3)	❍	❍	❍	❍	❍
Setup your environment (library dependencies, providers etc.) correctly (4)	❍	❍	❍	❍	❍
Understand which sequence of method calls from the identified API is needed (5)	❍	❍	❍	❍	❍
Understand which parameters need to be passed to the API method calls (6)	❍	❍	❍	❍	❍
Identify which provider to use (7)	❍	❍	❍	❍	❍
Understand the underlying implementation of API calls (8)	❍	❍	❍	❍	❍
Understand the error	❍	❍	❍	❍	❍

messages provided by the API (9)					

What do you think would be a useful tool/technology/idea that can further help you complete your cryptographic tasks more correctly, efficiently, etc.?

Further comments